Valetax

Anti-Money Laundering Manual

VALETAX GLOBAL LIMITED

November 2025

Definitions

"Beneficial Owner" means the natural person or natural persons, who ultimately own or control the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The Beneficial Owner shall at least include:

(a) In the case of corporate entities:

i. An individual who is an ultimate beneficial owner of the legal person, partnership or legal arrangement, whether or not the individual is the only beneficial owner; and

ii. An individual who exercises ultimate control over the management of the legal person, partnership or legal arrangement, whether alone or jointly with any other person or persons.

(b) For the purposes of paragraph (a) above, it is immaterial whether an individual's ultimate ownership or control of a legal person, partnership or arrangement is direct or indirect.

(c) An individual is deemed not to be the beneficial owner of a company, the securities of which are listed on a recognised exchange.

"Company" means Valetax Global Limited, which is registered in St. Vincent and the Grenadines with registration number 23398 BC 2016 and with its registered office address located at Suite 305, Griffith Corporate Centre, Beachmont, P.O. Box 1510, Kingstown, St. Vincent and the Grenadines.

"Employee" means any person engaged to perform work for the Company, whether under a contract of employment or contract for services.

"Law" means the Anti-Money Laundering and Terrorist Financing Regulations, 2014 as amended from time to time.

"Politically Exposed Person (PEP)" means (a) a foreign politically exposed person; (b) a domestic politically exposed person; (c) a person who is or has been entrusted with a prominent function by an international organisation. It also includes natural persons who are or have been entrusted with prominent public functions within the State or in a foreign country, including their immediate family members or persons known to be close associates.

The following persons are considered to hold prominent public functions:

i. Heads of state, heads of government and senior politicians

ii. Senior government, judicial or military officials

iii. Members of the boards of central banks

iv. Ambassadors and chargés d'affaires.

v. Senior executives of state-owned corporations.

vi. Important political party officials.

For persons linked to an international organisation, the following are considered to exercise prominent functions:

i. Directors and deputy directors.

ii. Members of the board or governing body.

iii. Other members of senior management.

Immediate family members of a PEP include a spouse, a partner, children and their spouses or partners, parents, grandparents and grandchildren or siblings.

For the purposes of this definition, **"partner"** means a person living in a domestic relationship similar to that between husband and wife; or a person whose relationship is considered equivalent to that of a spouse under the applicable law of any jurisdiction.

Close associates of a PEP include any person known to maintain a close business relationship with the PEP or able to conduct substantial financial transactions on their behalf; any person known to have joint beneficial ownership of a legal person or legal arrangement with the PEP or other close business relations; any person who has sole beneficial ownership of a legal person or legal arrangement that is known to have been established for the benefit of the PEP.

When determining whether a person is a close associate, the Company is required to consider only information in its possession or information that is publicly known and/or available.

"Money Laundering" means the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it allows them to maintain control over those proceeds and ultimately, to provide a legitimate cover for their source of income. Failure to prevent the laundering of the proceeds of crime, permits criminals to benefit from their actions, thus, making crime a more attractive proposition.

Applicable Legislation

- Financial Intelligence Unit Act, Cap. 174 of the Revised Laws 2009
- Exchange of Information Act, Cap. 146 of the Revised Laws 2009
- Mutual Assistance in Criminal Matters Act, Cap. 177 of the Revised Laws 2009
- Proceeds of Crime Act, 2013
- Anti-Money Laundering and Terrorist Financing Regulations, 2014
- Anti-Terrorist Financing and Proliferation Act, 2015
- Anti-Money Laundering and Terrorist Financing (Amendment) Regulations, 2017
- Anti-Money Laundering and Terrorist Financing Code, 2017
- Anti-Terrorist Financing and Proliferation Amendment, 2017
- Immigration Restriction Amendment Act, 2017
- Proceeds of Crime Amendment Act, 2017

1. Introduction

Valetax Global Limited (hereinafter called "We" or the "Company") is registered in St. Vincent and the Grenadines with registration number 23398 BC 2016 and with its registered office address located at Suite 305, Griffith Corporate Centre, Beachmont, P.O. Box 1510, Kingstown, St. Vincent and the Grenadines.

St. Vincent and the Grenadines has established a comprehensive legislative and regulatory framework aimed at the prevention, detection and deterrence of money laundering, terrorist financing, and other financial crimes. This framework includes, among others, the Proceeds of Crime Act, the Anti-Money Laundering and Counter-Terrorist Financing Regulations, the Anti-Terrorist Financing and Proliferation Financing Act, the Financial Intelligence Unit Act, together with applicable guidelines, codes and directive issued by the competent authorities. These legislative measures reflect international best practices and take into account the 40 Recommendations of the Financial Action Task Force (FATF) and the 19 Recommendations of the Caribbean Financial Action Task Force (CFATF), demonstrating St. Vincent and the Grenadines' commitment to maintaining a robust AML/CFT regime and combating the proceeds of crime.

2. Money Laundering Process

Despite the variety of methods employed, the money laundering process is accomplished in three (3) basic stages, which may comprise transactions by the launderers that could alert a financial institution to criminal activity:

- Placement – The process of placing, through deposits or other means, unlawful cash proceeds into traditional financial institutions.
- Layering – The process of separating the proceeds of criminal activity from their origin through the use of layers of complex financial transactions, such as converting cash into traveller's checks, money orders, wire transfers, letters of credit, stocks, bonds or purchasing valuable assets, such as art or jewellery. All of these transactions are designed to disguise the audit trail and provide anonymity.
- Integration - The process of using an apparently legitimate transaction to disguise the illicit proceeds, allowing the laundered funds to be disbursed back to the criminal. Different types of financial transactions, such as sham loans or false import/export invoices, can be used. If the layering process is successful, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

The three (3) basic steps may occur as separate and distinct phases or may occur simultaneously or, more commonly, they may overlap. How the basic steps are used depends on the available laundering mechanisms and requirements of the criminal organisations.

Certain points of vulnerability have been identified in the laundering process which the money launderer finds difficult to avoid and where his activities are, therefore, more susceptible to being recognised specifically.

3. Money Laundering Methods

There are numerous money laundering methods. However, the most common are the following:

(a) **Structuring -** It involves many individuals who deposit cash into back accounts or buy bank drafts in amounts under EUR 10,000 to avoid the reporting threshold.

(b) **Money Services and Currency Exchanges -** Money services and currency exchanges provide a service that enables individuals to exchange foreign currency that can then be transported out of the country. Money can also be wired to accounts in other countries. Other services offered by these businesses include the sale of money orders, cashiers' cheques, and travellers' cheques.

(c) **Asset Purchases with Bulk Cash –** Money launderers may purchase high value items such as cars, boats or luxury items such as jewellery and electronics. Money launderers will use these items but will distance themselves by having them registered or purchased in an associate's name.

(d) **Electronic Funds Transfer –** Also referred to as a telegraphic transfer or wire transfer, this money laundering method consists of sending funds electronically from one city or country to another to avoid the need to physically transport the currency.

(e) **Postal Money Orders –** The purchase of money orders for all cash allows money launderers to send these financial instruments out of the country for deposit into a foreign or offshore account.

(f) **Credit Cards –** Overpaying credit cards and keeping a high credit balance gives money launderers access to these funds to purchase high value items or to convert the credit balance into cheques.

(g) **Casinos –** Cash may be taken to a casino to purchase chips which can then be redeemed for a casino cheque.

(h) **Refining –** This money laundering method involves the exchange of small denomination bills for larger ones and can be carried out by an individual who converts the bills at a number of different banks in order not to raise suspicion. This serves to decrease the bulk of large quantities of cash.

(i) **Legitimate Business / Co-mingling of Funds –** Criminal groups or individuals may take over or invest in businesses that customarily handle a high cash transaction volume in order to mix the illicit proceeds with those of the legitimate business. Criminals may also purchase businesses that commonly receive cash payments, vending machine companies. They will then, insert criminal funds as false revenue mixed with income that would not otherwise be sufficient to sustain a legitimate business.

(j) **Value Tampering –** Money launderers may look for property owners who agree to sell their property, on paper, at a price below its actual value and then accept the difference of the purchase price "under the table". After holding the property for a period of time, the launderer then, sells it for its true value of USD 2 million.

(k) **Loan Back –** Using this method, a criminal provides an associate with a sum of illegitimate money, and the associate creates the paperwork for a loan or mortgage back to the criminal for the same amount, including all of the necessary documentation. This creates an illusion that the criminal's funds are legitimate. The scheme's legitimacy is further reinforced through regularly scheduled loan payments made by the criminal and providing another means to transfer money.

4. Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The FATF is therefore a "policy-making body" created in 1989 that works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. The FATF has published 40 + 9 Recommendations in order to meet this objective. The third Anti-Money Laundering Directive is in line with the FATF Recommendations.

FATF monitors members' progress in implementing necessary measures, reviews money laundering and terrorist financing techniques and countermeasures and promotes the adoption and implementation of appropriate measures globally. In performing these activities, FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism.

5. Procedures for preventing Money Laundering and Terrorist Financing

The Company shall establish and maintain a comprehensive Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) framework designed to identify, assess, monitor, and mitigate the risks of money laundering and terrorist financing. These procedures ensure that the Company complies with applicable laws and regulations and that effective internal controls are implemented across all business lines.

5.1. Appointment of Compliance Officer

The Company's Board of Directors shall appoint a Compliance Officer, at managerial level, who is suitably qualified and competent employee of the Company, with sufficient authority, seniority, and autonomy to discharge their AML/CFT responsibilities.

Senior Management shall ensure that the Compliance Officer has:

- Direct and unrestricted access to all relevant records, data, and systems in a timely manner.
- Adequate resources, including time, technology and staffing.

- The ability to make final decisions regarding the filing of suspicious activity reports (SARs) with the Financial Intelligence Unit (FIU).

Where appropriate, based on the Company's size, operational complexity or geographical reach, the Board may appoint one or more Deputy/Assistant Compliance Officers. Their roles shall be clearly defined and communicated to all employees.

5.2. Duties and Responsibilities of the Compliance Officer

The Compliance Officer is responsible for establishing, implementing and maintaining an effective AML/CFT framework in accordance with the Proceeds of Crime Act, AML/CFT Regulations, FIU Guidance Notes and applicable international standards. At a minimum, the duties include:

(a) Development of AML/CFT Systems, Procedures and Internal Controls

- Designing and maintaining internal AML/CFT policies, procedures, controls and practices based on the Company's risk profile.
- Explicitly allocating AML/CFT responsibilities across departments and ensuring accountability.
- Ensuring AML/CFT risk mitigation is considered when developing new products, technologies or entering new markets.

(b) Customer Acceptance and Risk Management

- Developing the Customer Acceptance Policy and submitting it to the Board for approval.
- Preparing and updating the AML/CFT Risk Management and Procedures Manual.
- Overseeing the application of risk-based measures relating to customers, products, services, jurisdictions, delivery channels and technology.

(c) Monitoring and Testing Compliance

- Monitoring adherence to AML/CFT policies and controls across departments.
- Conducting periodic reviews, testing effectiveness, and performing onsite/desk-based assessments.
- Identifying deficiencies and ensuring prompt remediation, escalating issues to Senior Management or the Board as needed.

(d) Internal Suspicion Reporting and SAR Decision-Making

- Receiving internal disclosures of unusual or suspicious transactions from employees.
- Evaluating internal reports, gathering additional information where necessary and documenting assessments.
- Making the final determination on whether a SAR should be filed with the FIU.
- Liaising directly with the FIU and, where necessary, law enforcement agencies.

(e) Risk Assessment and Ongoing Review

- Maintaining customer risk categorisation and updating based on new information or behavioural changes.

- Identifying and assessing emerging risks relating to new customers, products, delivery channels and technologies.
- Evaluating AML/CFT controls of third parties when reliance or outsourcing is used.

(f) Training and Awareness

- Developing and implementing the annual AML/CFT training plan.
- Providing guidance and continuous awareness to employees on AML/CFT matters.
- Assessing the adequacy and effectiveness of training delivered.

(g) Reporting to Senior Management and the Board

At least annually, and more frequently where required based on risk, the Compliance Officer shall submit a formal AML/CFT Compliance Report to Senior Management and the Board. The report shall include, at a minimum:

- Assessment of the effectiveness of AML/CFT systems and internal controls
- Identified deficiencies and remediation actions taken or required
- Statistics on internal suspicion reports received and SARs submitted to the FIU
- Training conducted and participation levels
- Updates on legislative / regulatory changes and required implementation steps
- Risk assessment updates, including high-risk jurisdictions and FATF-listed countries
- Resource requirements, where applicable.

Senior Management and/or the Board shall promptly implement corrective measures arising from the Compliance Officer's report.

5.3. Board of Directors' Responsibilities

The Board of Directors oversees the Company's governance framework and is accountable for ensuring that effective measures are in place to prevent money laundering, terrorist financing and proliferation financing. The Board ought to ensure that the Company maintains robust systems and controls aligned with the legal and regulatory requirements of St. Vincent and the Grenadines and applicable international standards.

Accordingly, the Board shall:

- Define, document and approve the Company's AML/CFT policy principles and ensure that these are communicated to the Compliance Officer.
- Appoint a Compliance Officer and, where required, Assistant Compliance Officers, and formally establish their roles, responsibilities and reporting lines.
- Approve the customer acceptance policy.
- Approve the AML/CFT Risk Management and Procedures Manual and ensure that it is disseminated to all relevant employees.
- Ensure that the Company implements effective internal systems, controls and procedures to manage AML/CFT risks.
- Ensure ongoing adherence to all regulatory and statutory AML/CFT obligations.

- Ensure that the Compliance Officer receives full, unrestricted and timely access to customer data, transaction records and all information necessary to perform investigative and reporting duties.
- Provide the Compliance Officer with adequate resources, including authority, personnel and technological tools, to perform the role effectively.
- Safeguard the Compliance Officer's autonomy, ensuring independence in the assessment and reporting of suspicious transactions.
- Establish and maintain an internal reporting chain that enables employees to promptly escalate suspicious activity to the Compliance Officer.
- Ensure that all employees are informed of the identity and responsibilities of the Compliance Officer and any designated assistants.
- Review and evaluate the Compliance Officer's Annual Report and take timely corrective action to address identified weaknesses or recommendations.

Furthermore, the Board of Directors shall determine, document and approve the general AML/CFT policy principles of the Company relating to the prevention of money laundering, terrorist financing and proliferation financing. The Board shall communicate these principles to the Compliance Officer.

The Compliance Officer is responsible for preparing the AML/CFT Risk Management and Procedures Manual in accordance with the policy principles approved by the Board. The Manual shall be submitted to the Board for review and formal approval.

Following approval, the Compliance Officer shall ensure that the Manual is communicated to all relevant employees involved in managing, monitoring or controlling customer activity, and to those responsible for implementing AML/CFT measures, procedures and internal controls.

5.4. Internal Policies, Procedures and Controls

The Company shall maintain written AML/CFT policies, procedures and internal controls adequate to prevent and detect money laundering and terrorist financing, taking into account:

- The nature, size scale and complexity of operations.
- The diversity of activities, products, services and delivery channels
- Customer characteristics, transactional activity, and applicable risk levels.

AML/CFT policies and controls must be risk-sensitive and proportionate to the Company's exposure to money laundering and terrorist financing risk.

Where the Company operates as part of a group or has branches, subsidiaries or representative offices in order jurisdictions, it shall:

- Communicate its AML/CFT standards to all related entities.
- Ensure that entities apply AML/CFT measures equivalent to those required in St. Vincent and the Grenadines.
- Maintain group-wide information sharing for the purposes of customer due diligence, ongoing monitoring, record keeping and risk management.
- Ensure adequate safeguards for the confidentiality of shared information.

Where a foreign jurisdiction prohibits the application of equivalent AML/CFT measures, the Company must inform the FIU promptly, take additional risk mitigation measures as directed by the FIU, and terminate the relationship, if adequate mitigation cannot be achieved.

5.5. Reporting of Suspicious Activity

All employees must promptly report any knowledge or suspicion of money laundering or terrorist financing to the Compliance Officer. Where necessary, employees in foreign branches or offices must report suspicious activity related to the Company to the Compliance Officer in St. Vincent and the Grenadines.

The Company shall ensure that internal reporting procedures are clearly communicated and documented.

5.6. Employee Screening and Fitness and Propriety

The Company shall ensure that all relevant employees meet high standards of competence, integrity and suitability for their roles in accordance with the Company's AML/CFT policies and procedures. For the purposes of this Policy, a relevant employee is one who in the course of their duties has, or may have, access to information relevant to determining whether funds or assets may be the proceeds of crime, or whether a person may be involved in money laundering or terrorist financing; or is involved in implementing, supporting, or monitoring the Company's compliance with AML/CFT requirements.

Where functions are outsourced to a third party, the Company must implement procedures to ensure that the third party applies effective screening controls to confirm the competence and integrity of individuals performing AML/CFT related work on behalf of the Company.

To ensure that all relevant employees are fit and proper for their positions, the Company shall, at a minimum:

- Obtain and verify appropriate employment or character references at the time of recruitment, where applicable;
- Verify employment history, academic qualifications and any professional memberships, where applicable;
- Request and verify information regarding any regulatory or disciplinary actions taken by a regulator or professional body; and
- Request and verify information relating to any criminal convictions or confirmation of no convictions, which may include obtaining a police clearance certificate from the relevant jurisdiction(s).

The Company shall maintain written or electronic records of all steps taken to verify the suitability of employees, including copies of evidence obtained during the screening process. Where full verification cannot be completed, the Company must document:

- The reason why the required information could not be obtained;
- A risk-based justification for proceeding with the appointment; and
- Any alternative measures taken to mitigate potential risks.

6. Independent Audit

The Company shall maintain an independent audit function to periodically assess the effectiveness of its AML/CFT framework. The audit must evaluate the design and operational effectiveness of the Company's AML/CFT policies, procedures and internal controls. The audit shall also be conducted at least annually and more frequently where:

- Weaknesses, gaps or deficiencies are identified; or
- Senior Management deems it necessary based on the Company's risk assessment and exposure to ML/TF risks.

Depending on the size and risk profile of the Company, the audit may be performed by an internal audit function, the Compliance Department or another qualified internal unit, provided that the audit is carried out independently of general operational or financial audits. A separate dedicated department is not required; however, AML/CFT audit activities must remain independent, objective and clearly distinct from operational functions or business decision-making.

The audit function must be appropriately staffed and resourced to ensure effectiveness and shall:

- Review and validate the Company's risk assessment process, including risk ratings assigned to customers, products, services, transactions, geographic exposure, delivery channels and outsourcing arrangements.
- Assess the adequacy and effectiveness of AML/CFT policies, procedures and internal controls, including:
    i. Risk assessments and risk mitigation measures;
    ii. Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) procedures;
    iii. Ongoing monitoring of customer relationships and transactions;
    iv. Procedures for detecting, escalating and reporting suspicious activity;
    v. Record-keeping and document retention practices; and
    vi. Reliance on outsourcing arrangements.
- Test compliance with applicable legislation, regulations and guidance issued in St. Vincent and the Grenadines.
- Perform sample testing of transactions and activities, with particular emphasis on higher-risk areas.
- Evaluate employee understanding of the Company's AML/CFT obligations, internal policies and procedures, and individual responsibilities in preventing money laundering and terrorist financing.
- Assess the adequacy and effectiveness of AML/CFT training and awareness programmes.

Findings, conclusions and recommendations resulting from the audit shall be documented and formally reported to Senior Management and the Compliance Officer. Senior Management shall ensure that any identified deficiencies are addressed promptly and that appropriate corrective measures are implemented.

7. Customer Due Diligence (CDD) and Identification Requirements

The Company shall apply Customer Due Diligence ("CDD") and customer identification measures in accordance with Section 11 of the AML/CFT Regulations, the Proceeds of Crime Act and the Guidance Notes issued by the FIU of St. Vincent and the Grenadines.

The Company shall identify and verify the identity of each customer and, where applicable, the beneficial owner, prior to establishing a business relationship or conducting an occasional transaction. CDD also includes understanding the purpose and intended nature of the relationship and whether the customer's activities and transactions align with their expected profile, source of funds and overall risk classification.

CDD forms the basis for ongoing monitoring and enables the Company to determine whether a customer or transaction may pose a money laundering or terrorist financing risk.

7.1. CDD Application

The Company must identify and verify the customer's identity and beneficial ownership information in the following instances:

(a) Prior to establishing a business relationship or carrying out an occasional transaction. Verification must occur before account activation or allowing any trading or funding activity on the platform.

(b) Where suspicion exists that a transaction or relationship may involve money laundering or terrorist financing, irrespective of the amount involved, or where the Company has doubts concerning the adequacy or accuracy of previously obtained information.

(c) When dealing with customers seeking to trade in virtual assets or cryptocurrency-related products, which shall be treated as higher-risk and subject to Enhanced Due Diligence (EDD), consistent with the FIU guidance regarding higher-risk delivery channels.

(d) For existing customers, CDD must be refreshed at intervals determined by the Company's risk assessment; and at least once every five (5) years, as required under Section 11 of the Regulations.

Additional CDD is required when customer identification information changes, beneficial ownership changes, or a third party begins acting on behalf of the customer or there is a change in that third party's ownership structure.

7.2. Enhanced Due Diligence (EDD) and Enhanced Ongoing Monitoring

In cases where a client, product, service, delivery channel or transaction presents a higher risk of money laundering or terrorist financing, the Company shall apply EDD and Enhanced Ongoing Monitoring.

EDD consists of applying additional, proportionate measures to mitigate higher ML/TF risk and must, at a minimum, enable the Company to understand:

- The client's identity and beneficial ownership with a higher level of certainty;
- The source of funds, and where applicable, the source of wealth; and
- The nature, background and purpose of transactions or activities.

EDD and enhanced monitoring shall be applied in the following situations, at a minimum:

(a) Non-face-to-face or remote onboarding

Where the client is not physically present during onboarding, the Company shall perform at least one additional independent verification measure to mitigate impersonation and fraud risk and apply enhanced monitoring until verification has been fully completed, and risk has been reassessed.

(b) High-Risk Jurisdictions

When the client or a third party connected to the business relationship is linked to a country that is identified by FATF as high-risk or subject to calls for action, or is known for inadequate AML/CFT controls, corruption concerns, or strategic deficiencies.

(c) PEPs

EDD shall apply where the client, beneficial owner, third party or any individual acting on behalf of the client is a foreign PEP or a close associate or immediate family member of a foreign PEP.

(d) High-risk business models or ownership structures

EDD is required where the client relationship involves private banking or personal asset-holding vehicles, legal persons or arrangements with nominee shareholders or bearer shares, and complex or layered ownership structures obscuring beneficial ownership.

For EDD cases, the Company shall apply one or more of the following measures:

- Obtain additional or more recent identification documents or information;
- Obtain additional information on the purpose and intended nature of the relationship;
- Obtain information on source of funds and source of wealth;
- Increase frequency and depth of ongoing monitoring, including review of transaction patterns and limits;
- Obtain senior management approval prior to onboarding or maintaining the relationship.

7.2.1. Transactions favouriting anonymity

In cases where onboarding or transactional activity occurs through non-face-to-face channels, such as online platforms, telephone instructions, email, fax, or other electronic communication, the Company shall implement additional measures to verify the identity of the client and mitigate impersonation, identity fraud and anonymity risk, in line with the applicable legislation.

The Company shall ensure that reliable authentication methods and access controls are in place, including but not limited to:

- **Online Platform / Portal Access:** Multi-Factor authentication, unique client credentials and secure passwords;
- **Telephone Instructions:** Confirmation of identity through client-specific verification questions (e.g. date of birth, ID/Passport number, customer code);

- **Fax or Scanned Document Instructions:** Signature verification against the signature specimen maintained in the client's records.

These controls shall provide reasonable assurance that the Company is dealing with the legitimate account holder or an authorised representative.

7.3. Timing of Verification and Exceptional Circumstances

Verification of identity must be completed before establishing the business relationship. Subject to Section 11(4) of the Regulations, the Company may finalise verification after onboarding, only in circumstances where:

(a) Doing so is necessary to avoid interrupting the normal course of business,
(b) The ML/TF risk is demonstrably low, and
(c) Verification is completed as soon as reasonably practicable.

Where verification is allowed to be completed after account creation, appropriate safeguards shall be implemented, including preventing the customer from executing transactions, deposits, or withdrawals until verification is finalized.

Additionally, the Company shall conduct ongoing monitoring throughout the relationship0 in order to:

(a) Ensure transactions are consistent with the customer's business profile, risk classification and declared source of funds;
(b) Identify unusual or suspicious activity;
(c) Keep customer information up to date.

EDD shall be applied where higher ML/TF risk is identified, such as for PEPs, customer involved in virtual asset activities, complex ownership structures, or customers operating from high-risk or FATF-listed jurisdictions.

7.4. Failure tor Refusal to Complete CDD – Mandatory Decline or Termination

In accordance with Section 11(6) of the Regulations, the Company shall not establish a business relationship or execute any transaction if the client:

- Fails or refuses to provide the required identification or verification information;
- Provides information that is false, inconsistent or cannot be verified; or
- Otherwise prevents the Company from completing CDD.

Where a business relationship already exists and the Company is subsequently unable to complete identification or beneficial ownership verification, obtain required updated documentation during periodic reviews, or conduct adequate ongoing monitoring, then the Company shall terminate the business relationship.

Prior to termination, the Company may suspend account activity or restrict transactional capabilities until the required documents are received. No exceptions or overrides are permitted.

In all cases where CDD cannot be completed or where refusal to provide information gives rise to suspicion, the Compliance Officer shall assess whether the circumstances warrant the filing of an SAR with the FIU, in accordance with the applicable legislation.

7.5. Application of Customer Due Diligence and Identification Procedures

The Company shall apply CDD and customer identification procedures in accordance with the requirements set out under Section 6 of the AML/CFT Regulations, supported by the Proceeds of Crime Act and FIU Guidance Notes.

The Company shall identify each customer and determine whether the customer is acting on their own behalf or on behalf of a third party. Where a customer acts on behalf of a third party, the identity of that third party must also be obtained and verified.

In cases where the customer or related party is not a natural person, the Company shall identify all beneficial owners and take reasonable, risk-based measures to verify their identity. For legal entities, partnerships, trusts, foundations or similar arrangements, the Company shall obtain sufficient information to understand the ownership and control structure. Identification and verification are not required where ownership interests relate solely to individuals holding shares in a company listed on a recognised stock exchange.

Where a verification is required, the Company shall verify identity information through documents, data or information obtained from reliable and independent sources, in line with the Regulations. If an individual claims to act on behalf of a customer, the Company shall take reasonable measures to confirm that the individual is authorised to do so. The Company then, shall identify and verify the identity of that individual accordingly.

Before establishing a business relationship, or executing an occasional transaction, the Company shall obtain information on the purpose and intended nature of the customer relationship or activity.

For cryptocurrency related activities or high-risk situations, the Company shall understand the background and purpose of any transaction that appears:

(a) Complex;
(b) Unusually large;
(c) Conducted in an unusual manner;
(d) Without a clear economic or lawful purpose;

If the activity involves a high-risk third country, the Company shall apply enhanced monitoring, which may include increasing the frequency of controls and reviewing transaction patterns in greater detail.

7.6. Ongoing Review and Updating of Client Identification Information

The Company shall ensure that all client identification records and economic profile information remain accurate, complete and up to date throughout the business relationship. The Compliance Officer is responsible for maintaining current client information, consistent with Section 11 of the AML/CFT Regulations.

To that end, CDD information shall be reviewed on a risk-based frequency, including:

- **High-Risk Clients:** at least every twelve (12) months;

- **Medium-Risk Clients:** at least every twenty-four (24) months;
- **Low-Risk Clients:** at least every thirty-six (36) months.

The outcome of each review shall be recorded and filed in the client's profile or electronic file, together with any updated documentation collected.

If, at any time during the business relationship, the Company identifies missing, outdated or insufficient information, the Compliance Officer shall promptly request and collect additional documentation to update the client's profile.

Additional review and due diligence shall be triggered if any of the following events occur:

(a) A transaction that is inconsistent with the client's regular activity or declared economic profile;

(b) A material change in the client's legal or organisational structure, including but not limited to:

- Change of directors or authorised signatories
- Change in shareholders or beneficial ownership
- Change of registered address, trade name or trustees (where applicable)
- Opening of additional accounts or new financial instruments / services

(c) Any circumstance that may alter the client's risk rating or expected transaction behaviour.

Where triggered, the Compliance Officer shall reassess the client's risk classification and ensure that the client's written economic profile reflects the most recent information.

7.7. Client Identification Requirements by Client Type

7.7.1. Natural Persons

When onboarding natural persons, the Company shall obtain and verify government-issued identification (i.e. valid passport or national identity card) and retain certified true copies of relevant pages. It will also determine whether the client currently holds or has held a prominent public function within the previous twelve (12) months, and whether they are a family member or close associate of a PEP. Where doubt exists regarding the authenticity of documentation, the Company may seek verification through embassies, consulates or reputable financial institutions in the client's country of residence.

7.7.2. Joint Accounts

For joint accounts, the identity of every individual with ownership or signing authority over the account must be verified in accordance with the procedures applicable to natural persons. Each party shall be treated as an individual client for CDD purposes.

7.7.3. Unions, Societies, Clubs, Provident Funds and Charities

When onboarding a non-profit or unincorporated association, the Company shall verify the legitimacy and purpose of the organisation by requesting governing documents (e.g. constitution, rules, registration certificates, etc.). Additionally, the Company shall obtain a list of members of the governing body or management committee and verify the identity of all individuals authorised to operate the account using natural-person CDD procedures.

7.7.4. Partnerships, Unincorporated Businesses and Other Non-Legal Entities

For partnerships and unincorporated businesses, the Company shall identify and verify the identity of partners, beneficial owners and authorised signatories, obtain certified true copies of the partnership registration, wherever applicable, evidence of business and if applicable, partnership agreements. Finally, the Company shall also obtain information regarding the nature, size and purpose of the business, and documentation needed to construct the client's economic profile.

7.7.5. Legal Persons (i.e. Companies)

Prior to establishing a business relationship, the Company shall confirm that the legal person is validly incorporated and active. Measures include company searches, registry checks or commercial data sources to confirm that the entity is not dissolved, struck off or in liquidation.

The Company shall collect and verify:

General Information:

- Purpose of the business relationship
- Registered office and contact details
- Anticipated transactional activity (i.e. turnover, volume, funding sources, destination of transfers)
- Names and verification of authorised signatories (where persons identified must be verified using natural-person CDD standards)
- Shareholders and nominee shareholders (where persons identified must be verified using natural-person CDD standards)

Economic Profile / Risk Assessment:

- Company name and tradename
- Country of incorporation and registered office address
- Identification of all Ultimate Beneficial Owners (UBOs) (where persons identified must be verified using natural-person CDD standards)
- Directors / managers / signatories (where persons identified must be verified using natural-person CDD standards)
- Nature of business, activities, products and services

- Financial information (i.e. audited accounts or management accounts if available)
- Group structure, if applicable

Verification Documentation

- Certificate of Incorporation
- Memorandum and Articles of Association
- Certificate of Directors, Secretary and Registered Office
- Shareholder Register
- UBO Declaration (if different from shareholders)
- Board resolution authorising account opening and signatories
- Certificate of Good Standing (for foreign or recently incorporated entities)
- Proof of registered office address (i.e. utility bill, bank statement, etc.)
- Publicly available company information (e.g. website, brochures, etc.)
- Registry search confirming active status
- Financial statements or management accounts (where necessary)

If any shareholder or director is a legal entity, the same procedure shall apply until natural persons (UBOs) are identified.

7.7.6. Investment Funds, Mutual Funds and Regulated Financial / Investment Service Firms

The Company may establish relationships with entities that are regulated in an EEA member state or equivalent jurisdiction or licensed and supervised for AML/CFT purposes. The Company then, shall obtain proof of licensing or authorisation, which will be verified with the issuing authority or reliable sources, documentation on ownership and control structure, and identification of beneficial owners, investment managers, administrators and custodians.

7.7.7. Nominees and Agents

Where a nominee or agent acts on behalf of a third person, the Company shall identify and verify the nominee / agent, identify and verify the third person they represent and obtain a valid and signed authorisation agreement governing the relationship.

7.8. Risk-Based Application for CDD and Monitoring

In accordance with Section 13 of the AML/CFT Regulations and the relevant FIU Guidance Notes, the Company shall apply CDD and ongoing monitoring measures using a documented Risk-Based Approach (RBA). The purpose of the RBA is to ensure that the nature and extent of due diligence measures applied are proportionate to the assessed money laundering or terrorist financing risk associated with each client, product, service, delivery channel or geographic exposure.

Under the Risk-Based Approach, the Company shall:

- Assess the risk level of each business relationship or occasional transaction by considering factors such as customer type, ownership structure, source of funds, jurisdiction, delivery channel and transaction features.
- Determine the extent of CDD measures and the level of ongoing monitoring to be applied based on the identified level of risk, ensuring that higher-risk situations are subject to increased scrutiny and enhanced due diligence.
- Maintain a documented client risk assessment, supported by CDD information and any additional data collected during the onboarding process.
- Review and update client information periodically and revise the client's risk rating as necessary, particularly when new information is obtained, or unusual activity is detected.

When preparing and updating client risk assessments, the Company shall consider at minimum the following risk dimensions:

(a) Client Risk – nature of client, ownership structure (if applicable) and occupation/activity
(b) Product/Service Risk – type of product or service being offered or used
(c) Delivery Channel Risk – onboarding method (remote or face-to-face), intermediaries involved
(d) Country / Geographic Risk – whether the client or counterparties have connections to high-risk or FATF-identified jurisdictions.

The Company ought to be able to demonstrate to the competent Authorities that the extend of the CDD applied is appropriate and justified, having regard to the specific ML/TF risks identified; and that adequate information has been obtained and retained to support the client risk assessment and ongoing monitoring decisions.

8. Customer Risk Categorisation

The Company shall classify all clients into risk categories based on a documented, risk-based assessment. The classification considers factors such as jurisdiction, business activity, delivery channels, products utilised, ownership structure and any other relevant risk indicators. Risk categorisation enables the Company to determine the level of due diligence, monitoring and approval required in accordance with the applicable legislation.

8.1. Restricted Jurisdictions (No Onboarding Permitted)

The Company does not establish business relationships with individuals or entities located in, or having significant connections to, jurisdictions that are sanctioned, subject to FATF calls for action, or otherwise prohibited by law or regulatory constraints.

The following jurisdictions are strictly prohibited:

- Iran
- Democratic People's Republic of Korea (i.e. North Korea)
- Myanmar
- United States of America

No exception or escalation mechanism applies. Any attempted onboarding of such clients shall be declined and, where appropriate, assessed for suspicious activity reporting to the FIU.

8.2. Low-Risk Clients

The following may be categorised as low risk where the likelihood of money laundering or terrorist financing is demonstrably minimal:

(a) Regulated financial or credit institutions subject to AML/CFT supervision in St. Vincent and the Grenadines or in an equivalent jurisdiction;
(b) Public authorities or governmental bodies in St. Vincent and the Grenadines;
(c) Companies whose securities are listed on a recognised stock exchange and subject to disclosure requirements ensuring transparency of beneficial ownership.

Prior to assigning a low-risk rating, the Company must obtain sufficient evidence that the client meets the criteria an ensure that no adverse information is identified during screening.

8.3. Medium-Risk Clients

Clients that do not meet the criteria for either Low-Risk or High-Risk classification shall be categorised as Medium-Risk or Normal-Risk clients. Such clients shall remain subject to standard CDD and ongoing monitoring, consistent with the Company's risk-based approach.

8.4. High-Risk Clients

Clients that present a higher risk of money laundering or terrorist financing shall be classified as "High-Risk" and are subject to EDD, as outlined under Section 7.6. of this Manual. This includes, but is not limited to:

- PEPs, including family members and close associates;
- Clients associated with high-risk jurisdictions, other than the fully restricted countries defined in Section 8.1.;
- Clients with complex ownership or control structures, private asset-holding vehicles, trusts or nominee arrangements;
- Clients engaging in virtual asset or cryptocurrency-related activities.

The rationale for assigning a High-Risk classification shall be documented in the AML system or risk register.

9. Reliance on Third Parties for Client Identification and Due Diligence

The Company may rely on third parties to perform certain elements of CDD. Reliance may only relate to:

- Identifying the client and verifying their identity;
- Identifying the beneficial owner and verifying their identity;
- Obtaining information on the purpose and intended nature of the business relationship.

Reliance on third party does not transfer accountability. The Company shall remain fully responsible for ensuring compliance with AML/CFT requirements and for determining whether the information provided is adequate.

9.1. Eligible Third Parties

The Company may rely on an introducer, intermediary or other third party only where:

(a) The third party is a regulated or supervised entity subject to AML/CFT obligations consistent with FATF standards; and

(b) The third party formally agrees to be relied upon for CDD purposes.

Eligible third parties include:

- Regulated financial or credit institutions;
- Foreign financial institutions or service providers subject to equivalent AML/CFT supervision;
- Licensed professionals (e.g. lawyers, accountants, corporate service providers) who are supervised for AML/CFT compliance.

Reliance must be documented and approved by the Compliance Officer.

9.2. Documentation and Access to Information

Before placing reliance on a third party, the Company shall ensure that the third party agrees to:

- Provide, without delay, certified true copies of all identification documents and beneficial ownership information obtained during CDD; and
- Make all CDD information and supporting records available to the Company upon request.

The Company shall obtain sufficient documentation to enable verification of the client's identity, beneficial ownership structure and intended purpose of the relationship.

9.3. Assessment and Monitoring of Third Parties

Prior to reliance, the Company shall assess and document that the third party:

- Is registered and authorised in its jurisdiction;
- Is subject to AML/CFT supervision and regulatory oversight;
- Applies standards at least equivalent to those of St. Vincent and the Grenadines.

Reliance is permitted only at onboarding for initial identity verification. Any additional information required for ongoing monitoring, enhanced due diligence or updating the client's economic profile shall be obtained directly from the client or beneficial owner, not from the third party.

10. Suspicious Transactions and Activities

The Company shall remain vigilant in identifying transactions or behaviours that may indicate money laundering or terrorist financing. A transaction is considered suspicious when it appears inconsistent with the client's known profile, declared source of funds or expected activity. Suspicious indicators may appear individually or in combination, and the presence of any such indicator warrants closer examination and escalation to the Compliance Officer.

10.1. Red Flags Associated with Money Laundering

Examples of transactional and behavioural indicators that may suggest money laundering include:

- Transactions that are unnecessarily complex, lack clear economics rationale or do not match the client's business activity or financial profile.
- Frequent transfers to or from foreign accounts involving jurisdictions with weak or inadequate AML/CFT controls.
- Use of third parties to fund or receive payments without clear business justification
- Reluctance by a client to provide required identification, beneficial ownership or source-of-funds information, or providing information that is inconsistent, misleading or difficult to verify.
- Frequent changes to contact details, authorised signatories or corporate structure without reasonable justification.
- Evidence suggesting that a legal entity or ownership structure is being used to obscure beneficial ownership.

These indicators are not exhaustive. The Company must apply professional judgment and escalate concerns to the Compliance Officer for assessment.

10.2. Terrorist Financing Indicators

Unlike money laundering, funds used in terrorist financing may originate from legitimate sources. Indicators of possible terrorist financing include:

- Frequent international transfers with no business justification, particularly involving non-profit entities or jurisdictions commonly associated with geopolitical instability or terrorism.
- Donations or transfers to individuals or organisations that are not aligned with the stated purpose or size of the organisation.
- Unusual or unexplained increase in financial activity within non-profit organisations.

10.3. Cryptocurrency / Virtual Asset ML/TF Risk Indicators

Given the Company's exposure to virtual asset activity, enhanced monitoring applies to cryptocurrency-related transactions. Examples of red flags include:

(a) Transaction Behaviour

- Structuring transactions into smaller amounts to avoid reporting or monitoring thresholds.
- Rapid inflow and outflow of cryptocurrency with no logical business purpose.
- Sudden conversation of cryptocurrency to multiple asset types or withdrawal immediately after deposit.

(b) Patterns / Volume Indicators

- A new wallet funded with a large initial deposit that is immediately traded or withdrawn.
- Multiple incoming transfers from unrelated wallets followed by consolidation into a single outgoing transfer.
- Transactions conducted at an apparent loss due to unnecessary conversion fees.

(c) Anonymity Indicators

- Use of privacy coins or mixing / tumblr services to obscure transaction origin.
- Use of proxy servers, VPNs, TOR, or multiple IP addresses in different locations to access the account.
- Wallets linked to darknet markets, gambling sites or exchanges with weak AML/CFT controls.

(d) Sender / Recipient Indicators

- Multiple accounts opened using the same IP address, device or identification details.
- Clients who refuse to provide information on the relationship with counterparties.
- Transactions originating from high-risk jurisdictions, IPs or exchanges, not subject to AML/CFT supervision.

(e) Source of Funds

- Cryptocurrency sourced from ICOs, platforms, or exchanges lacking AML/CFT controls.
- Use of multiple credit/debit cards or repeated attempts to fund or withdraw through cards associated with unrelated individuals.

(f) Geographical Risk

- Clients interacting with exchanges or service providers located in jurisdictions known for weak AML/CFT frameworks or subject to FATF notices.

10.4. Required Internal Actions

When a suspicious activity or indicator is identified, employees must refrain from alerting or "tipping-off" the client of any concerns regarding the transaction or ongoing assessment. The employee must promptly escalate the observation to the Compliance Officer through the Internal Suspicion Report process and continue monitoring the client's activities and transactions until further instructions are provided. Upon receiving the report, the Compliance Officer will evaluate the information and determine whether the circumstances warrant filing an SAR with the FIU.

11. Client Screening and Sanctions Monitoring – Cleversoft

The Company utilises **Cleversoft** as part of its CDD and ongoing monitoring framework. WorldCompliance is an automated screening solution used to identify whether a prospective or existing client appears on sanctions lists, has been involved in criminal activity, or is classified as a PEP, in accordance with AML/CFT Regulations and FATF requirements.

Screening is performed before the establishment of a business relationship and prior to granting any trading or transactional activity. Screening is conducted on identity documentation and personal data submitted during onboarding. When documents include Machine Readable Zone (MRZ) data, the system may also assist in detecting potential document fraud.

The screening process enables the Company to determine whether the client:

- Appears on sanctions, law enforcement or watchlists (e.g. terrorism financing, money laundering, fraud, etc.);
- Is classified as a PEP or is a family member or close associate of a PEP;
- Is associated with adverse media or negative reputational indicators.

Where a client is identified as a PEP, the following actions apply:

- The Compliance Officer shall review and approve onboarding prior to completion of verification.
- The client shall be recorded on the Company's Internal PEP / Watch List.
- The relationship will be subject to EDD and ongoing monitoring.

In events where a client match indicates involvement in criminal activity or inclusion on international sanctions or law enforcement lists (e.g. terrorism, money laundering, fraud) the onboarding request must be declined immediately, any existing account must be blocked without delay, and the Compliance Officer shall assess whether an SAR must be filed with the FIU.

No client flagged for criminal activity or sanctions risk shall be onboarded under any circumstances.

12. Record Keeping

The Company shall maintain complete and accurate records of client identification, due diligence, transactional activity and ongoing monitoring, in accordance with the AML/CFT Regulations, the Proceeds of Crime Act and FIU Guidance Notes.

12.1. Documents and Data to be Retained

The Company shall retain the following records, in physical or electronic format:

(a) Client identification records, including copies of evidential material used to verify identity and beneficial ownership, and any related supporting documents.

(b) Due diligence and risk assessment records, including:
- Risk classification (e.g. low/medium/high risk)
- Results of periodic reviews of client files
- Documentation concerning any reliance on third parties for CDD

(c) Transactional records, including:
- Details and evidence of all business relationships and transactions
- Accounting and financial records, including records relating to cryptocurrency transactions.

(d) Correspondence records, including communication with clients or persons related to the business relationship.

(e) Internal AML documentation, including Internal Suspicion Reports and Internal Evaluation Reports as well as SARs filed with the FIU.

All records must be stored in a manner that enables the Company to reconstruct individual transactions and demonstrate compliance with due diligence and monitoring obligations.

12.2. Retention Period

All records shall be retained for at least five (5) years from the date the business relationship ends, or from the date of completion of a transaction, whichever occurs later. Where ongoing investigations, FIU requests, regulatory requirements or legal proceedings require extended retention, the Company shall retain the records for the duration specified by the relevant authority.

12.3. Availability and Access

Records shall be readily retrievable and accessible without undue delay. The Company shall ensure that all documentation, including electronic records, can be produced promptly to the FIU, supervisory authorities or law enforcement agencies upon request, to enable them to discharge their statutory duties.

12.4. Certification and Language of Documentation

Documents obtained from clients must be original or certified true copies. Where the certification is performed by a third party outside the Company or outside the trusted network of approved intermediaries, the Company may require notarisation or apostille, depending on jurisdictional requirements. If documents are issued in a language other than English, a certified translation must accompany the original document.

12.5. Oversight and Management Responsibility

The Compliance Officer is responsible for managing and maintaining the Client Risk Classification Register, ensuring that it reflects the client's risk level, identifier, date of onboarding and date of the most recent review. The register must be updated as soon as new information is obtained or when material changes occur in the client's structure, jurisdictional exposure or transactional behaviour. The Compliance Officer shall also ensure that all record-keeping obligations are consistently applied and that the Company's retention procedures remain aligned with legal and regulatory requirements.

13. Employees' Obligations, Training and Awareness

All employees have a legal and regulatory duty to support the Company's AML/CFT framework. Employees must immediately report any knowledge, suspicion or reasonable grounds for suspicion of money laundering or terrorist financing activity. Reports shall be submitted promptly to the Compliance Officer using the Internal Suspicion Report process (i.e. **Appendix 2**).

Employees are expressly prohibited from informing or "tipping-off" any client regarding internal reviews, suspicion or potential reporting to the authorities.

Upon receipt of an Internal Suspicion Report, the Compliance Officer reviews and evaluates the information, assesses it against available records and other relevant data, and documents the assessment in an Internal Evaluation Report (i.e. **Appendix 3**). If, following the evaluation, the Compliance Officer determines that an SAR shall be submitted, the Compliance Officer will prepare and file the report with the FIU without delay (i.e. **Appendix 4**).

Failure by an employee to report a suspicion or information that may be material to detecting money laundering or terrorist financing may result in personal criminal liability under applicable AML/CFT legislation.

13.1. Employee Training and Awareness Programme

The Company maintains a comprehensive and ongoing AML/CFT training programme to ensure that employees understand their legal obligations, the Company's internal policies and procedures and how to identify and respond to potential money laundering or terrorist financing activities.

The Compliance Officer is responsible for designing, implementing, and maintaining the training programme, including determining which departments and employees require specialised or additional training based on the nature of their duties and level of exposure to AML/CFT risk. Training is provided to new employees during onboarding and to all relevant employees on a recurring basis. The programme covers regulatory requirements, internal reporting procedures, red-flag indicators and developments in AML/CFT methodologies, including those related to virtual assets and cryptocurrency-based risks.

The Compliance Officer continuously evaluates the adequacy and effectiveness of training delivered, ensuring that employees remain informed of emerging typologies, trends and regulatory changes. The Compliance Officer must maintain the necessary expertise and technical knowledge to enhance internal procedures and support employees in recognising, preventing, and responding to activity that may be linked to money laundering or terrorist financing.

Appendix 1: Client Acceptance Policy on a Risk-Based Approach

The Company's client acceptance policy is prepared by the Compliance Officer following detail assessment of the risks faced by the Company. In this regard, the Company shall apply appropriate measures and procedures, on a risk-based approach, so as to focus its efforts in those areas where the risk of money laundering and terrorist financing appears to be higher.

Risk Criteria

The Compliance Officer shall identify, record and evaluate three (3) main risk criteria when assessing the extent of money laundering and terrorist financing risks. Based on the extent and the combination of the given risk criteria, the overall risk of a client will be quantified as either High, Medium or Low.

The Compliance Officer shall consider the following criteria:

i. Country or Geographic Risk
ii. Client Risk
iii. Products / Services Risk
iv. Delivery Channel Risk

Risk Indicators

The Compliance Officer shall analyse the above risk criteria into different risk indicators as shown in the following table:

Risk Criteria	Risk Indicator
Customer Risk	Customer characteristics/behavior/History
	Shareholder /Director / Beneficial Owner / Auth. Representative Characteristics
	Customer Business
	Customer ownership structure
	Duration of Business relationship
	Business activity / Expected yearly transaction turnover
Product and Service Risk	Transaction Types (cash/size)
	Payment Methods Used By Customer
	Transfer of Funds to Different Institutions/persons/third parties
	Product/service Types
Country/Geographic Risk	Country/Geographic Risk
Delivery Channel	Delivery Channel

Risk Variables

For each risk indicator, the Compliance Officer shall identify various “risk variables”, as shown in the following table:

Risk Criteria	Risk Indicator	Risk variables
Customer Risk	Customer characteristics/behaviour/History	Is there any apparent financial/commercial rationale for the customer buying the product/service?
		The origin of wealth and/or source of funds cannot be easily verified
		Requests to associate undue levels of secrecy (unwillingness to provide information on the beneficial owners)
		Accounts for "gatekeepers" (accountants, lawyers, or other professionals) for their clients
		Reliance for KYC and AML matters on the gatekeeper
		Number of related accounts
		SAR Filed Previously
		CTR Filed Previously
	Customer Business	Weapon manufacturers
		Art and antique dealers
		Dealers in high value or precious goods
		Real estate agents
		Unregulated charities
		Unregulated "non for profit" organisations
		Remittance houses
		Exchange houses
		Casinos
		Betting
		Gabling related
		Money transfer agents
		Bank note traders
		Cash intensive business
	Customer ownership structure	Complex business ownership structures
		Transparency structure
		Bearer shares
		Incorporated in offshore centres
	Duration of Business relationship	D < 1 year
		1 year < D < 3 Years
		D > 3 years
	Expected yearly transaction turnover	Turn < 100,000
		100,000 < Turn < 1,000,000

		1,000,000 < Turn < 5,000,000
		5,000,000 < Turn < 20,000,000
		Turn > 20,000,000
Product and Service Risk	Transaction Types	Cash transactions
		Size of transaction
	Product/service Types	Do the products allow/facilitate payments to third parties
		Can the product features be used for money laundering or terrorist financing, or to fund other crime
		Do the products/services intended to render the customer deliberately anonymous to the financial institution
	Payment Methods Used By Customer	Bank Transfer
		Neteller / Skrill / Dinpay
		Safecharge
		Credit Cards
		Web Money
	Transfer of Funds to Different Institutions/persons/third parties	No Movement
		MF = 1 Institution
		1 Inst. < MF < 3 Inst.
		3 Inst. < MF < 5 Inst.
		MF > 5 Inst.
Country/Geographic Risk	Country/Geographic Risk	FATF jurisdictions which have endorsed the 40+9 recommendations
		Transparency International (CPI)
		MONEYVAL
		UN Security Council Sanctions Committees
		International Monetary Fund (IMF)
		Office of Foreign Assets Controls (OFAC)
		Transactions to/from high-risk jurisdictions
		Low Risk jurisdiction
Customer Risk	Shareholder /Director / Beneficial Owner / Auth. Representative Characteristics	Certified true copy of proof passport is obtained
		Color ID is obtained
		Certified true copy of recent proof of Residence is obtained
		Clean World - Check report
		Validation of Passport
		Bank / Legal advisor / Accountant reference letter is obtained

		Is the customer included in the relevant list of persons subject to financial sanctions which are issued by the UN
		Country of Origin
Delivery Channel	Delivery Channel Risk	Face to Face Client
		Introduced by a person related to the Company (i.e., employee, shareholder, service provider)
		Non-face to face client

Risk Classification Model:

For each client / account, the Compliance Officer analyses the different risk criteria mentioned above and assign scores and weights to the various risk variables and risk indicators. The Compliance Officer shall combine the risk rating rom each risk criteria at the client level to determine the overall risk level by completing the table below. Additionally, the Compliance Officer has the authority, at their absolute discretion not to follow the standard procedure described in this section, if they believe that by doing so, for a specific client, the assigned classification will not be correctly reflected.

Risk Levels	Unique Combinations	Customer Risk	Product/ Transaction Risk	Geographic Risk
Risk Level 1	1	H	H	H
	2	H	H	N
	3	H	N	H
	4	N	H	H
Risk Level 2	5	H	N	N
	6	N	H	N
	7	N	N	H
Risk Level 3	8	N	N	N

H = High Risk
N = Neutral Risk

Using this model, there are three (3) Risk Levels. Risk Level 1 represents accounts with the highest risk.

Risk Level 1 (Higher Risk Client): Accounts with two or three (2 or 3) High-Risk designations
Risk Level 2 (Normal Risk Client): Accounts with one (1) High-Risk designation
Risk Level 3 (Normal Risk Client): Accounts with no High-Risk designations

Based on the criteria described above, clients will be categorised in the following three (3) categories: (a) Low Risk, (b) Medium Risk and (c) High Risk.

Criteria for accepting new clients

This Company shall only establish a business relationship with a new client once all required information and verification procedures have been completed in accordance with this Client Acceptance Policy and Appendix 1 of this Manual.

(a) Clients not Eligible for Onboarding

All prospective clients are assessed individually by the Compliance Officer. Before approving a new application, the Compliance Officer must confirm that the information and documentation submitted by the applicant is complete, accurate, authentic and consistent. This includes verifying the client's identity, evaluating the credibility and legitimacy of the information provided, and considering whether the applicant is exposed to illegal or criminal activity risk. Where appropriate, database checks may be conducted to assess financial soundness, adverse media, sanctions exposure or other integrity risk indicators.

Applications shall be rejected where required documentation is missing, where a client refuses or fails to provide information, or where the information is incomplete, inconsistent, or raises suspicion about the client's financial integrity. The Company will also reject applications where there are reasonable grounds to believe that the client may be involved in illegal or criminal activities, or where the client's background or behaviour presents unacceptable risk.

(b) Assessment and Documentation of Client Information

The Compliance Officer shall perform a structured assessment of each prospective client, including analysis of identity information, ownership structure, business activities and expected transactional behaviour. This assessment aims to determine the legitimacy of the client's source of funds and wealth, whether the proposed activity is consistent with the client's profile, and whether any factor suggests a potential link to money laundering, terrorist financing or other unlawful activity.

During the evaluation, particular attention is paid to red flags such as reluctance to provide requested information, inconsistencies or contradictions in the documentation provided, or information that does not appear to be credible. The results of this assessment are documented in a due diligence report prepared by the Compliance Officer. For corporate clients, this assessment also identifies the beneficial owner(s), individuals with decision-making authority, sources of funds and any operational or legal limitations relevant to the client. For individuals, the report records the ownership of funds, origin of funds, intended use and any applicable restrictions.

If no adverse indicators are identified, the Compliance Officer may proceed with onboarding and the execution of relevant agreements. If, however, the evaluation suggests possible involvement in illicit activity, the Compliance Officer shall decline the relationship and, where applicable, file an SAR with the relevant authority without informing the client.

No orders or transactions may be executed for a client before the completion of the verification, assessment and approval process. The Company strictly prohibits the opening of anonymous accounts or accounts held on behalf of fictitious or undisclosed beneficiaries.

(c) Approval of Client Acceptance Policy

The Client Acceptance Policy is prepared by the Compliance Officer and submitted to the Board of Directors for review and approval. The Policy is reviewed periodically to ensure continued alignment with regulatory requirements and the Company's risk appetite.

Appendix 2: Internal Suspicious Report for ML and TF

INFORMER'S DETAILS	
[redacted]	
Name:	Tel: .....
Department:	Fax: .....
Position:	
CLIENT'S DETAILS	
Name:	
Address:	
....	Date of Birth: .....
Tel:	Occupation: .....
Fax:	
Details of Employer:	
Passport No.:	Nationality: .....
ID Card No.:	
Other ID Details: .....……	
INFORMATION/SUSPICION	
Brief description of activities/transaction:	..... ……

....

..... ……

Reason(s) for suspicion:

.....

.....	.....	……
Informer's Signature		Date
.....		……..….
FOR COMPLIANCE OFFICER'S USE		
Date Received:	Time Received:	Ref.....
Reported to MOKAS: Yes/No ……..	Date Reported:	Ref.....

Appendix 3: Internal Evaluation Report for Money Laundering and Terrorist Financing

Reference: ..... Client's Details: .....

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

INQUIRIES UNDERTAKEN (Brief Description)

.....

.....

.....

ATTACHED DOCUMENTS

....

....

....

COMPLIANCE OFFICER'S DECISION

.....

.....

FILE NUMBER .....

COMPLIANCE OFFICER'S SIGNATURE DATE

....

Appendix 4: Compliance Officer's Report to the FIU for Combating Money Laundering

I. GENERAL INFORMATION

Financial Organization's
Name: .....
Address where customer's account is
kept: .....
.....
Date when a business relationship established or
occasional transaction was carried
out: .....
Type of account(s) and number(s):
.....

II. DETAILS OF NATURAL PERSON(S) AND/OR LEGAL ENTITY(IES) INVOLVED IN THE SUSPICIOUS TRANSACTION(S)

(A) NATURAL PERSONS

	Beneficial owner(s) of the account(s)	Authorized signatory(ies) of the account(s)
Name(s):	.....	.....
	.....	.....
Residential address(es):	.....	.....
	.....	.....
	.....	.....
	.....	.....
Business address(es):	.....	.....
	.....	.....
	.....	.....
Occupation and Employer:	.....	.....
	.....	.....

	.....	.....
Date and place of birth:	.....	.....
	.....	.....
	.....	.....
	.....	.....
Nationality and passport number:	.....	.....
	.....	.....
	.....	.....

(B) LEGAL ENTITIES

Legal entity's name, country and date of incorporation: .....

.....

.....

Business address: .....

.....

.....

Main activities: .....

.....

	Name	Nationality and passport number	Date of birth	Residential address	Occupation and employer's details
Registered Shareholder(s)	1. .... 2. .... 3.	....	....	....	....
Beneficial Owner(s) (if different from above)	1. .... 2. .... 3.	....	....	....	....
Directors	1. .... 2. .... 3. .... 4.	....	....	....	....
Authorized signatory(ies) of the account(s)	1. .... 2. .... 3.	....	....	....	....

.....

III. DETAILS OF SUSPICIOUS ACTIVITIES

Details of suspicious activities should be given

1. ……
   ……
   ……
   ……
   ……
2. ……
   ……
   ……
   ……
   ……
3. ……
   ……
   ……
   ……
   ……

4. **<u>Knowledge/suspicion of money laundering or terrorist financing</u> (please explain, as fully as possible the knowledge or suspicion connected with money laundering or terrorist financing)**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

5. <u>Other information</u> – Other services provided to the customer(s)

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

Compliance Officer's Signature Date

…… ……