Anti-Money Laundering Policy and Procedures

Version: 1.5

August 2024

Contents

Definitions and Acronyms

"AML" means Anti-Money Laundering.

"AML Act" means Consolidated Anti-Money Laundering and Countering the Finance of Terrorism Act, 2020 with regulations and subsequent amendments.

"AML Regs" means Anti-Money Laundering and Countering the Finance of Terrorism Regulations, 2020 with subsequent amendments.

"BO" means Beneficial Owner and shall have the same meaning set out under Section 3 of the Consolidated Beneficial Ownership Act, 2020

"CDD" means Customer Due Diligence procedure as set out in this Policy.

"CFT" means Combating the Financing of Terrorism.

"CO" means Compliance Officer of the Company, who is the senior officer within the Company responsible for the establishment of the relevant procedures in relation to the AML/CFT and reporting directly to the Board of Directors of the Company.

"Company" means ForexVox (Seychelles) Financial Services Ltd.

"EDD" means Enhanced Due Diligence procedure as set out in this Policy.

"FATF" means a Financial Action Task Force (on Money Laundering), an intergovernmental organization founded on the initiative to develop policies to combat money laundering and terrorism financing, and to maintain certain interest.

"FIU" means Financial Intelligence Unit in Seychelles.

"FSA" means the Financial Services Authority in Seychelles.

"KYC" means Know Your Customer, standards designed to protect the Company against fraud, corruption, money laundering and terrorism financing.

"PEP" means Politically Exposed Person and shall have the same meaning set out under Section 36(2) of the AML Act.

"Policy" means this Anti-Money Laundering Policy and Procedures.

"SDD" means Simplified Due Diligence procedure as set out in this Policy.

"SCR" means Seychelles Rupees.

“STR/SAR” means Suspicious Transaction Report/Suspicious Activity Report, a report that shall be submitted by the Company to the FIU under section 48 of the AML Act.

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

Background Documents Reference

1. Consolidated Anti-Money Laundering and Countering the Finance of Terrorism Act, 2020 with regulations and subsequent amendments.
2. Anti-Money Laundering and Countering the Finance of Terrorism Regulations, 2020 with subsequent amendments.
3. Consolidated Beneficial Ownership Act, 2020 with regulations and subsequent amendments.
4. Consolidated Beneficial Ownership Regulation, 2020 with subsequent amendments.
5. Prevention of Terrorism Act, 2004
6. Prevention of Terrorism (Implementation of UNSCR on Suppression of Terrorism) Regulations, 2015
7. Prevention of Proliferation Financing Regulations, 2021
8. Prevention of Terrorism (Implementation of United Nations Security Council Resolutions on Suppression of Terrorism) (Amendment) Regulations, 2022
9. AML/CFT Procedures for reporting entities in Seychelles, 2015
10. Beneficial Ownership Guidelines, 2020.
11. Consolidated Securities Act, 2007 with regulations and subsequent amendments.
12. Code for Compliance Function, 2023
13. Code on Outsourcing of Compliance Function, 2022.
14. Any other applicable Guidelines, Circulars or Notices issued by the FSA, FIU or other competent authority.

1. Introduction

1.1. Policy

ForexVox (Seychelles) Financial Services Ltd. is a Company incorporated and registered under the laws of Seychelles with Company number 8430368-1. The Company is licensed and regulated as a Securities Dealer by the Financial Services Authority under Securities Dealer license number SD142.

The primary purpose of this Policy is to document the approved approach and guidance of the Company, relating to:

- Financial crime – Preventing Company's association with money laundering, terrorism financing, fraud, and bribery and corruption;
- Establishing new customer relationships; and
- Monitoring of existing customer relationships.

In addition, the Policy identifies and provides guidance on implementing the key internal procedure and controls in support of the AML and CFT framework and confirms the determination of Company's Board of Directors and senior management to prevent potential cases of money laundering and financial of terrorism, and implement measures to counter financial crime.

This Policy is prepared in accordance and with the purpose to comply with the applicable laws and regulations pertaining to AML and CFT both within Seychelles and those issued by international bodies and organizations, such as FATF. This Policy shall be communicated to all Directors, managers, and 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.

Any amendments and/or changes to this Policy shall be approved by the Board of Directors of the Company and later communicated to the FSA.

1.2. AML statement

The Board of Directors and senior management are responsible for assessing money laundering risk and ensuring appropriate implementation of risk-based approach and relevant procedures within the Company. The Board of Directors fully supports the Seychelles AML and CFT regime and has zero tolerance for criminal use, or misuse, of Company's services or products in furtherance of money laundering.

The Board of Directors is committed to ensuring that:

- The relevant policy principles of the Company in relation to the prevention of the money laundering and terrorism financing are determined, documents by the means of this Policy and approved;
- The risk of the Company being used as a vehicle for money laundering or terrorism financing is minimized;
- The senior officer who possesses relevant knowledge, skills and expertise is appointed to act as a CO of the Company, or such function is being outsourced to such provider as approved by the FSA, according to the Code on Outsourcing of Compliance Function, 2022;
- Appropriate knowledge and awareness are maintained within the Company on all levels, of the Seychelles AML requirements and relevant laws and regulations;
- Where transactions suspected to involve money laundering are recognized, these will be reported to the appropriate authorities, including any linked to persons or entities suspected of being involved in or supporting acts of terrorism financing;
- All employees within the Company are aware of this Policy and its requirements in respect to obligation to report any suspicions transactions and activities, and are also aware about the CO to whom they report, and reporting procedure;
- Should a customer of the Company come under investigation by law enforcement, the Company will be able to provide its part of any relevant audit trail, in respect of transactions or information about the customer, held by the Company.

The Board of Directors expects all Directors, managers, and employees of the Company to:

- Comply with this Policy;
- Attend and complete relevant training provided by the Company or any third-party provider, including AML training;
- Be alert to money laundering, fraud and other forms of financial crime, including bribery and corruption, and financial sanctions risk;
- To report incidents or suspicions (as per this Policy); and
- Ensure timely reporting to the Compliance Officer of all money laundering suspicions identified in any transaction or activity associated with Company's customers.

It should also be the responsibility of the Board of Directors of the Company to assess and approve the Annual Report of the CO, determine measures to be undertaken deemed appropriate under the circumstances to remedy and rectify any weaknesses and/or deficiencies identified, or address any areas of risk.

As a regulated firm, the Company is required, to:

- Appoint a Compliance Officer;
- Assess money laundering risk associated with the Company's customers;
- Implement risk-based approach, which serve to reduce the risk of the business being used for money launderers and terrorism financing or other financial crime, including procedures linked to:
  - Account opening, CDD, KYC and related procedures;
  - Ongoing monitoring arrangements;
  - Record retention;
- Maintain records, including records of all prescribed CDD measured and all transaction undertaken for the period of no less than required by relevant laws;
- Report suspicious transactions and activities to the FIU, and make necessary disclosures;
- Provide relevant training to its Directors, managers, and employees.

2. Money laundering

2.1. What is money laundering?

Money laundering is a process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. Money laundering enables criminals to maintain control over their illicit proceeds and ultimately to provide legitimate cover for the illegal source of the illicit proceeds. This means that proceeds from criminal activities is converted into assets that gives it an appearance of legitimate money. Money laundering is an international scourge and the failure by the authorities to prevent the laundering of the proceeds of crime will enable criminals to benefit from their illegal activities, thereby making crime a viable proposition.

The Financing of Terrorism is defined as an offence established when a person "by means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they will be used in full or

in part, in order to carry out a terrorist act or activity".
Terrorist financing is a unique form of financial crime. Unlike money laundering, which is finding dirty money that is trying to be hidden; terrorist financing is often clean money being used for lethal purposes.

The Company should follow and apply the provisions of the law which reflect the FATF international standards to prevent, detect and combat money laundering and terrorist financing. It is, therefore, imperative that all relevant personnel understand the nature of money laundering and terrorism financing and take the necessary measures to protect themselves.

There is no specific method of laundering money. Despite the variety of methods employed, the laundering process is accomplished in three basic stages which may comprise transactions by the launderers that could alert a financial institution to criminal activity:

- Placement: is the physical deposit of criminal proceeds derived from illegal activity i.e. entering the collected cash into the financial circuits (payment in cash, exchange of bills, manual exchange, travelers' checks, casino checks, etc.).

- Layering: is the separation of criminal proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity i.e. transfer between accounts, drawing of checks, foreign transactions etc.

- Integration: is the provision of apparent legitimacy to the proceeds of crime. If the layering process has succeeded, integration places the laundered proceeds back into the economy in such a way that they appear as normal (business) funds or other assets i.e. investing funds in lawful investments (stores, leisure activities, real estate, but also companies of all types, etc.

When dealing with customers (or new applicants for business) you need to be alert to the possibility that customers, their counterparties or others (with or without the customer's knowing participation) may try to launder money using the firm's services – by way of layering or integration.

2.2. Money Laundering Offences

AML Act includes various criminal offences related to money laundering. Under Section 3(1) of the AML Act a person is guilty of money laundering if:

- **he or she directly or indirectly acquires property from the proceeds of criminal conduct;**

- **knowing or believing that property is or represents the benefit of criminal**

conduct or being reckless as to whether the property is or represents such benefit, the person, without lawful authority or excuse (the proof of which shall lie on the person):

- converts, transfers or handles the property, or removes the property from the Republic of Seychelles;
- conceals or disguises the true nature, source, location, disposition, movement or ownership of the property or any rights associated with the property; or
- acquires, possesses or uses the property.

In the case of terrorism financing, Part III of the Prevention of Terrorism Act, 2004 includes offences related to involvement in provision or collection of funds or property for terrorism financing, or other types of offence.

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

Criminal conduct is often terming predicate offence. The AML Act take a threshold approach in defining criminal conduct as any act or omission against any law in the Republic of Seychelles or elsewhere that is punishable on conviction to a term of imprisonment, fine or to both.

2.3. Failing to disclose

Persons employed in the regulated sector commit an offence if they fail to make a disclosure in cases where they have knowledge or suspicion, that money laundering is occurring.

Where the Company or any of its Directors, managers, and employees, as well as any of its agents fail without lawful excuse to comply with the requirements of the AML Act, the Company or any of its Directors, managers, and employees, as well as any of its agents may be guilty of offences under the AML Act.

A failure to disclose offence is committed if an individual fails to make a report comprising the required disclosure as soon as is practicable in the form of an internal report to the CO of the Company.

The obligation to make the required disclosure arises when:

- A Director, manager, or employee knows or suspects, or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering;

- The information or other matter on which a suspicion is based came to a Director, manager, or employee in the course of business in the regulated sector;

- A Director, manager, or employee either can identify that other person is involved in money laundering, or has information concerning the whereabouts of the laundered property or the information he has may assist in identifying the person or the whereabouts of the property (the laundered property is that which forms the subject matter of the known or suspected money laundering).

When submitting an internal report to the CO:

- CO have a duty to make disclosures, if they have knowledge, suspicion or reasonable grounds to suspect money laundering or terrorism financing, as a consequence of an internal report;

- A CO may commit an offence if he fails to pass on reportable information in internal reports that he has received, as soon as is practicable, to the FIU.

2.4. Tipping-off

Tipping Off occurs where without lawful excuse, an act is carried out which notifies or discloses to a customer or unauthorized third parties information or that fact that a report has been made to the FIU under the AML Act or that an investigation is taking place and the disclosure is likely to prejudice any investigation that might be conducted following the report referred to. A tipping-off offence may not be committed if the person did not know or suspect that the disclosure was likely to prejudice any investigation that followed.

2.5. What are the money laundering risks

Execution only brokers carry out transactions in securities with regulated market counterparties, as agent for underlying customers. Execution only transactions are carried out only on the instructions of the customer.

Some execution only brokers deal with high volumes of low value customers transactions, whereas others direct their services towards higher net worth customers, and thus have fewer customers. Customers may adopt a variety of trading patterns. The Company is offering no advice and may have little, or no knowledge of a customer's motives.

Customers are also free to spread their activities across a variety of brokers for perfectly valid reasons and often do so. Each broker may therefore have little transaction history from which to identify unusual behavior. Many brokers provide execution only services on a non-face-to-face basis, including via the Internet.

In view of the above, while broking may be considered lower risk than some financial products and services, the risk is not as low as providing investment management services to the same type of customers in similar jurisdictions. Money laundering and terrorism financing can pose numerous risks to the Company. There are our major areas of risks as follows:

1. **Regulatory risk:** represents the risk of regulatory actions or sanctions being taken against the Company as a result of the failure to comply with applicable laws and regulations if the field of AML and CFT.

2. **Reputational risk:** represents the risk that the Company's reputation within the financial services industry in general, and its representation before its customers, partners, counterparties, potential employees and general public could be impaired by risk events.

3. **Operational risk:** represents the risk that any part of Company's services or operations will fail because of any adverse effect of human failure and/or system error which might result in a risk event.

4. **Liquidity risk:** represents the risk that the Company will not be able to meet its financial obligations as they arise due to any fines or sanctions imposed on the Company after occurrence of the risk event.

3. Who is the customer for AML purposes

The typical customers for execution only retail brokers are individuals. However, customers also include solicitors, accountants, as well as trusts, companies, charities etc.

The Company shall classify customers into various risk categories and based on the risk perception decide on the acceptance criteria for each category of customer. Where the customer, an account must be opened only after the relevant due diligence and identification measures and procedures have been carried out, as set out in this Policy. No account shall be opened in anonymous or fictitious name(s).

4. New customers

4.1. Customer identification and due diligence process

At a high level the Company will undertake the following:

- Customer Due Diligence is undertaken for all Company's customer. The

Company shall obtain and verify evidence of ID documents and Proof of Residence to fulfil the Anti-Money laundering requirements. Furthermore, additional Enhanced Customer Due Diligence shall be performed on a risk-based approach.

- Check whether the customer is a resident or a national of a noted “high risk” country, and then apply the required Enhanced Due Diligence according to the adopted risk-based approach if this if applicable;

- Check whether the customer is a resident or a national of a noted “restricted territory”, and then refrain from establishment or immediately terminate a business relationship with such customer;

- A Sanctions List check will be carried to check whether the customer is on the financial sanctions register or is a Politically Exposed Person.

The Company may after carrying out risk management procedures, to include but not limited to, limitation to the number, types or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for the type of relationship, complete the verification of the customer due diligence measures after the establishment of a business relationship if:

- this is necessary so as not to interrupt the normal conduct of business, such as —
  - non-face-to-face business;
  - securities transactions;
- there is no reasonably determined and justified suspicion of money laundering or terrorism financing activities.

Provided that the customer due diligence measures are completed as soon as practicable, no later than within 30 days from the date of commencement of a business relationship, which might be the date of the first financial transaction, or first trade executed by such customer.

4.2. Verifying customer’s identity

Reasonable steps must be taken to check the customer’s identity to show that they are who they claim to be and if applicable that they are trading for a legitimate purpose.

All new customers must provide sufficient information for verifying their identity and formal identification of personal ID and address will be completed by the Company. Guidelines for customer identification are provided below.

A risk-assessment will be undertaken to determine the extent of CDD required. In most cases, a standard CDD shall be applied, as described below in this Policy, however, in some cases this may provide for verification using an SDD process, or for higher risk situations, via the application of the EDD.

The CO has overall responsibility for ensuring the completion of necessary identity verification before determining whether, from an assessment of the customer's risk profile and nature of services required, approval to verify an account is deemed appropriate. This must be completed in all cases, without exception.

4.3. Simplified due diligence

Except where money laundering is suspected, SDD might be applied in certain cases.

The Company allows SDD measures to be applied in respect of:

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

The Company's SDD may include verifying the identity of the customer and the BO after the establishment of the business relationship, reducing the frequency of customer identification updates, reducing the degree of ongoing monitoring and scrutinising transactions, 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.

SDD might be applicable to customers, but should not automatically be assumed. Where an indicator or red-flag is present indicating a need for a higher degree of money laundering risk assessment, in such cases normal CDD or EDD must be applied (see below).

Whenever money laundering (or attempted money laundering) arrangement is suspected during the customer onboarding process, the CO must immediately be notified.

4.4. Enhanced due diligence

The term enhanced due-diligence or EDD officially means applying a rigorous and robust process of investigation over and above normal AML/KYC procedures, primarily

taking reasonable steps to verify and validate a customer's identity.

It's the regulatory obligation of a financial institution to understand and monitor a customer's profile, business, and account activity, specifically identifying irregular adverse information such as suspected fraud, money-laundering and/or terrorism financing. An EDD approach is designed to support actionable decisions to mitigate financial fraud, regulatory and reputational risk, as well as ensuring legal/regulatory compliance.

In addition to any situation which by its nature can present a higher risk of money laundering or terrorism financing, EDD must be applied in other specific cases as outlined in this Policy.

4.4.1. Non-face to face business

The Company's operating model is built around non-face-to-face contact with customers, predominantly via on-line contact. This means that the verification of information supplied by a customer on the account opening form, when confirming identity, must be based on reliable and independent sources.

Online identity verification is the preferred option for use with private individuals, though also can be used in other cases. It provides speed of response and corroboration, independent of a customer, about identity and existence. The Company shall maintain details of the approved provider(s) of electronic verification services.

Where personal identity is verified electronically, the customer's, in case of a private individual, or its directors', officers', shareholders' or beneficial owners', in case of a legal entity, full name and date of birth is to be used as the basis. Results of electronic verification must be consistent with a standard level of confirmation before being relied upon and also, used to assess the risk of impersonation fraud.

Whether the results might indicate a risk of identity theft, a need to apply EDD shall arise (on a risk-sensitive basis).

For non-face-to-face verification of customer identity, the Company will assess the need for any additional measure(s) to apply, in order to: mitigate the risk of impersonation fraud and money laundering; or to clarify any additional information that might be required when assessing applicant names against the Sanctions Lists.

Where necessary, the Company will cause additional measures to be applied, in order to compensate for data anomalies or higher risk indicators - for example, by applying one or more of the following:

- Ensuring that the first sums received from a customer originate from an account opened in the customer's name with a recognized bank;
- Verifying customer and payer details on the first payment received, should assist the Company to verify a customer's identity;

- Establishing telephone contact with the applicant (prior to opening the customer's account) via a home or business number which has been verified (electronically or otherwise), or holding a "welcome call" with the customer before transactions are permitted;
- Communicating with the customer at an address that has been verified;
- Conducting research into/about a customer's business operations, including research of news media and other open-source material on the Internet, or via subscription based service providers. Information collated may be useful to identify the reputation and standing of the customer, those who represent the customer and/or those who do business with the customer.

4.4.2. Verifying identity using customer documentation

Where on-line verification is not possible or impracticable, or fails this necessitates the receipt, review and handling of identity documents supplied by customers.

By way of example, on-line verification may not be possible, due to:

- Lack of availability of reliable data for use when confirming identity;
- A customer having moved address recently with little, if any, electronic footprint reflecting the address (or other details) provided to the Company;
- Data availability and content can vary by country, some being more or less contemporaneous than others.

4.4.3. Politically Exposed Persons

A PEP is defined as an individual who is or has been, during the preceding three years, entrusted with a prominent public function in Seychelles or any other country or an international body or organization. PEP also includes an immediate family member of a person referred to above or a close associate of a person referred to above.

PEP status itself does not incriminate an individual or entity. It does, however, put the applicant or an existing customer, or a beneficial owner, into a higher risk category.

Where, as a result of information identified by the Company's systems, information suggests that an applicant, existing customer, or a beneficiary is a PEP, this should immediately be reported to the CO for EDD purposes:

- The CO will cause any necessary additional due diligence to be conducted, in order to:
  - Assess the money laundering risk;
  - Determine whether it is appropriate to continue with the PEP relationship;
- The assessment will include scrutiny of the relevant person's personal

circumstances or change in status, as well as any identifiable complexity or structuring of the business relationship (e.g. involving companies, trusts or foreign jurisdictions), to ensure clarity about and legitimacy of any transaction(s).

- Although, by definition, an individual might cease to be a PEP after having left office for one year, a risk-based assessment is still required when determining whether appropriate monitoring of transactions or activity should continue to be applied at the end of this period. A longer period might be appropriate in order to ensure that the higher risks associated with an individual's previous position have adequately abated.

Having due regard to EDD findings and the need for on-going monitoring arrangements, prior to any approval of a PEP relationship:

- Approval should be obtained from the CO (or other senior manager) to establish (or continue) a customer relationship with a newly identified PEP;
- Adequate steps should to taken establish the source of wealth and source of funding to be involved in the customer relationship or transaction;
- The CO should ensure appropriate planning for conducting enhanced on-going monitoring if such a higher risk customer relationship is entered into or continued.

Where, a decision is made to continue with a PEP relationship the reasoning must be documented by the CO, and the CO should liaise with the business, to establish the:

- Nature and extent of information and on-going monitoring that should be captured and applied to the customer relationship; and
- Duration and frequency of monitoring required.

Where, a decision is made to decline a new application, or to discontinue an existing customer relationship, the CO will liaise with the business, to ensure that:

- Identifiable money laundering risk is assessed and dealt with appropriately (e.g. funds received, or to be received, or to be refunded/paid away);
- Appropriate steps are taken to exit the customer relationship;
- The customer is treated fairly and without prejudice to the firm's position.

4.5. Nature of business

Particularly with regards to corporate customers, but the principle applies also to non- business customers, sufficient information should be obtained and recorded, to provide a clear understanding of the applicant's nature of business. This will enable an assessment to be made of whether the purpose for which an account is wanting to be

established (see below), is consistent with the type of business being (or to be) transacted.

Understanding the customer's business enables opportunities to be identified for the Company to offer to provide a broader range of relevant services, as well as, understanding the customer's operational requirements for money transmission services.

4.6. Purpose of account

During a new customer registration process information should also be obtained, which reflects a good understanding of the intended use of Company's services and enables an assessment to be made of the money laundering risk. This applies to both individuals and companies. Additional information sought and details to be recorded against customer records, might include some of the following:

- A description of the customer's nature of employment;
- Expected source/origin of income and/or initial funds to be used in the account relationship (e.g. from a personal account in the customer's name);
- The level of income and total net worth;
- The anticipated transaction volumes, values and level of activity to be expected.

Recording the above information is a useful mechanism with which to aid deter and detect potential criminality, as well as providing a backdrop against which anomalies can be identified and/or account monitoring applied.

4.7. Red flags

Where a customer appears reluctant to provide information or is otherwise evasive in his answers, this may be indicative of concerns about commercially sensitive information, or a red flag to indicate money laundering risk. Where a doubt exists about information provided by a customer, or a concern is identified about lack of information, employees should contact the CO for advice.

These are generic examples of potential red-flags that could be highlighted within the industry as a whole:

- Attempts to obscure or avoid identifying personal identity or details of beneficial owners;
- Unwillingness to disclose the requested information;
- Customers whose lavish lifestyle appears to exceed known sources of income;

- Frequent changes to shareholders or Partners;
- Excessive or unnecessary use of nominees;
- Unnecessary granting of power of attorney;
- The involvement of companies in a transaction for no obvious commercial purpose;
- Subsidiaries having no apparent purpose;
- Uneconomic or inefficient structuring of transaction for no obvious commercial purpose, or which might be used by group structures for tax evasion purposes;
- Unusual, or out of the ordinary instructions;
- Repetitive or inexplicable changes to instructions;
- Use of bank accounts or funds transfers in several currencies without reason;
- Transfers of funds without evidence of underlying transactions;
- Sums paid exceed supporting information provided about goods/service costs;
- Customers appear disinterested in reducing commissions, exchange rate cost, etc.;
- Higher than expected funds transfer arrangements when considering the typical values and volumes expected of such customers;
- Corporate customers transferring large sums of money to or from overseas locations having no apparent link to the customer's nature of business;
- Customers paying round sum amounts to numerous bank accounts, or in round sum international transfer;
- Unexplained transfers of significant sums through several bank accounts.

In any instance where money laundering is suspected, details should immediately be notified to the CO, without alerting the customer or other person about whom a suspicion is held.

Failure or refusal by a customer to submit, before or during the establishment of a business relationship the requisite data and information for the verification of his identity and the creation of his economic profile, without adequate justification, constitutes elements that may lead to the creation of a suspicion that the customer is involved in money laundering or terrorism financing. In such an event, the Company shall not proceed with the establishment of the business relationship

while at the same time the CO considers whether it is justified under the circumstances to submit an STR/SAR to the FIU.

If, before or during the business relationship, a customer fails or refuses to submit, within a reasonable timeframe, the required verification data, and information the Company and the CO shall terminate the business relationship and close all the accounts of the customer, taking also into account the specific circumstances of the customer in question and the risks faced by the Company on possible money laundering and/or terrorism financing, while at the same time examine whether it is justified under the circumstances to submit a report to FIU.

4.8. Capturing information

When deciding whether or not to approve a new customer application, or when responding to queries about an existing customer, the Company should make an informed decision. It is important therefore, for employees having information relevant to a customer, or a customer's account, that the information content is available to the CO.

The following documents and records should be retained in accordance with procedures for record keeping, set out below:

- Telephone notes of discussions with customers;
- Correspondence or other documentation received from customers;
- Correspondence or other documentation received about customers.

5. CDD Requirements

5.1. Private individuals

The following information must be obtained for all applicants who are private individuals:

- Full name(s);
- Current residential address, city code, telephone number;
- Date of birth.

For an individual's ID document to be verified electronically electronic checking should use the person's full name and date of birth as a basis.

During the process of registration, each customer provides personal information,

specifically: full name, date of birth, residential address, phone number and city code, other information the Company deems necessary.

Identity shall be verified by reference to a document obtained from a reputable official source which bears a photograph.

Below is the list of valid documents the Company accepts for the purposes if ID verification:

- Passport;
- National ID Card;
- Driver's License;
- Any other government-issue document.

In order for the document to be accepted for ID verification it has to:

- contain full name, date of birth, photo, and citizenship of a customer, and also, where applicable: confirmation of the document validity (issue and/or expiry date), holder's signature;
- be valid as of the date of submission.

The current residential address shall be verified by the means of:

- a most recent utility bill (gas, water, electricity);
- bank or credit card statement;
- Tax Clearance Certificate or Tax Return;
- Police Character Certificate;
- Certificate of Residence or Residence Permit;
- other government-issued document that contains the current residential address and name of the customer at the Company's discretion.

Address verification for non- Seychelles resident customer might pose difficulties. However, passports or national ID cards will always be available. In such case, Company might accept a valid passport or national ID card for the purposes of current residential address registration if it contains residential address and the name of the customer, for customer from specific regions where it's practically complicated to obtain another proof of residential address.

With the exception of passport or national ID card, the document submitted to verify current residential address shall be not older than 6 (six) month from the date of submission.

For certain document types (such as national ID card, driver's license), both sides of the document must be submitted. Documents might be rejected if an image if unclear, blurred, cut, contains watermark, bears signs of use of graphic edit software, or any text cannot be read. Company might request the customer to resubmit the document or submit another document if it's not satisfied with the type of the document submitted or it's quality or has reasonably determined that its deemed necessary at its sole discretion.

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:

- occupation of the customer;
- the customer's investment objective and other related information concerning the customer's financial situation and needs;
- annual income, assets or net worth;
- other information the Company deems necessary for opening an account.

5.2 Private (or unlisted) company

Before entering into a business relationship with a private (or unlisted) company and / or those who represent it, appropriate verification checks must be applied where impersonation fraud may be a risk; particularly where the identity of those who represent the company is not verified face-to-face.

Steps must be taken to be reasonably satisfied that the person the Company deals with is properly authorized by the applicant (e.g. by way of Board resolution or a written authority addressed to the Company which is signed by the Partners issued on company letter head).

Where an entity is known or believed to be linked to a PEP (perhaps through a partnership or shareholding), or to a jurisdiction assessed as carrying a higher money laundering or terrorism financing risk, it is likely that this will put the entity into a higher risk category and EDD should be applied.

It is important that Company's records in relation to a private company applicant, enable it to reflect an understanding of the company's legal and ownership structure, and that sufficient additional information has been obtained on the nature of the company's business, and the reasons for seeking Company's services.

For company applicants, the Company must:

- Take reasonable steps to understand ownership and control of the customer. Information may need to be obtained from the official register or the

government-issued documents. Alternatively, the most recent audited accounts filed with the official register might provide sufficient detail about a company's operations, business activities and ownership structure;

- Obtain reliable information and assess the money laundering and terrorism financing risk associated with an applicant, the customer and business relationship, as well as the services sought and/or the transactions involved.

The following information must be obtained for all private company applicants:

- Full name;
- Registered number;
- Registered office in country of incorporation, and actual place of business, city code, telephone number;
- Business address.

A private company does not usually qualify for SDD. Under a risk-based approach, however, provided that confirmation is provided in writing by a reliable and independent source, the imposition of, say, regulatory obligations on an applicant firm (or customer) which is a private company, might be considered to provide an equivalent level of confidence in the company's public accountability.

Therefore, evidence that a corporate customer is subject to licensing and prudential regulatory regime of a statutory regulator in the EU (e.g. FCA, CySEC, CNMV, AMF or an equivalent jurisdiction), may be sufficient to satisfy identity verification requirements of such a customer.

For all private or unlisted companies where SDD cannot be applied, and therefore the following information/documents must be obtained:

- The company's existence should be verified from:
  - › either confirmation of the company's listing on a regulated market;
  - › or a search of the relevant company registry;
  - › or a copy of the company's Certificate of Incorporation;
- Memorandum and Articles of Association;
- Official registers confirming names and current residential addresses of all company's directors, partners, shareholders;
- Most recent audited accounts (if available);
- Most recent bank statement;

- Proof of the registered address of the company and proof of the business address, if different from the registered address;
- Proof of regulation (if applicable)
- The following information must also be obtained:
  - Names of all directors, partners and shareholders;
  - Names of all beneficial owners.

Where electronic verification is not possible (for either corporate or personal identity verification) and reliance is to be placed on documentation supplied by an applicant:

- Consideration should be given to whether any of the documents are forged;
- If they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

The registered or business address shall be verified by the means of:

- a most recent utility bill (gas, water, electricity);
- bank or credit card statement;
- Tax Clearance Certificate or Tax Return;
- Certificate of Registered Address;
- other government-issued document that contains the current residential address and name of the customer at the Company's discretion.

With the exception of Certificate of Registered Address, the document submitted to verify registered, or business address shall be not older than 6 (six) month from the date of submission.

The company's directors, partners, shareholders and BOs, as well as persons authorized to act on behalf of the company shall be verified in a same way as for the private individuals as described above in Section 5.1, in case if they are natural persons, and in the same way as described in this Section 5.2 in case if they are legal entities.

It will be ensured that:

- Standard evidence has been obtained and documented.
- Company identity has been reliably verified, either electronically or via reference to reliable source documents.
- The identity of appropriate directors and other company individuals has been verified.

- Authorized signatories and representatives dealing with the Company on behalf of the company have been properly authorized by the company.
- Details of the customer's 'nature of business and 'purpose of account' has been recorded.

5.2.1. Beneficial owners

In the case of a body corporate a beneficial owner includes any individual who ultimately own or control a customer or the natural person or persons on whose behalf a transaction is being conducted and includes those natural persons who exercise ultimate effective control over a legal person or a legal arrangement.

As part of collecting standard evidence, details of all individual beneficial owners owning or controlling the applicant company's shares or voting rights, even where these interests are held indirectly will be sought.

Verification requirements differ between a customer and a beneficial owner:

- Customer identity must be verified on the basis of documents, data or information obtained from a reliable and independent source;
- The obligation to verify beneficial owner identity is based on the Company taking risk-based and adequate measures, to be satisfied that it knows who the beneficial owner is.

In reviewing information obtained about a company's beneficial ownership, the Company will determine whether a need exists to seek further information about one or more beneficial owners; for example, whether to use records of beneficial owners in the public domain (if any), to arrange further contact with customers to seek relevant data, or to obtain the information otherwise.

5.2.2. Authorized signatories

For operational purposes, a list is likely to be maintained of those authorized to give instructions (on behalf of the company) for the movement of funds, along with an appropriate instrument authorizing one or more directors (or equivalent) to give the Company such instructions.

Where the identity of relevant company directors has been verified, the identities of individual signatories need only be verified if they do not appear on any of Register of Directors, Register of Shareholders or Register of Beneficial Owners. If, for example, all payment instructions are expected to originate from a customer's in-house accountant, who is not the director, a the Company shall verify the accountant's identity.

5.3. Companies listed on regulated markets

The Company is not required to verify the identity of a corporate customer whose securities are listed on a regulated European Economic Area market or equivalent overseas, which is subject to specified disclosure obligations.

This is due to the fact that such companies are publicly owned and generally accountable. The exemption also applies to companies that are majority-owned and consolidated subsidiaries of such companies.

If the market is outside the European Economic Area but is one which subjects companies whose securities are admitted to trading to disclosure obligations which are contained in international standards and are equivalent to the specified disclosure obligation in the European Union, similar treatment is permitted.

For companies listed outside the European Economic Area on markets which do not qualify for SDD, the standard verification requirement for private and unlisted companies should be applied.

5.4. Other customer types

The majority of Company's customers are expected to be individuals from Asia, South America and MENA who will use the Company's platform for investment on financial markets. It is unlikely that any of the customer types detailed below will arise, but for completeness these are included in this Policy. This section of Policy provides an overview of these customer types and their respective identification requirements.

5.4.1. Trusts

In some trusts and similar arrangements, instead of being an individual, the beneficial owner is a class of persons who may benefit from the trust. Where only a class of persons is required to be identified, it is sufficient to ascertain and name the scope of the class. It is not necessary to identify every individual member of the class.

For trusts or foundations that have no legal personality, those trustees (or equivalent) who enter into the business relationship with the Company, in their capacity as trustees of the particular trust or foundation, are customers on whom the Company must carry out full CDD measures. Following a risk-based approach, in the case of a large, well known and accountable organization, the Company may limit the trustees considered customers to those who instruct the Company. Other trustees will be verified as beneficial owners.

The beneficial owner of a trust is defined by reference to three categories of individual:

- Any individual who is entitled to a specified interest (that is, a vested, not a

contingent, interest) of the capital of the trust property;

- As respects any trust other than one which is set up or operates entirely for the benefit of individuals with such specified interests, the class of persons in whose main interest the trust is set up or operates;

- Any individual who has control over the trust.

The trustees of a trust will be beneficial owners, as they will exercise control over the trust property. In exceptional cases, another individual may exercise control, such as a trust protector, or a settlor who retains significant powers over the trust property. For the vast majority of trusts, either there will be clearly identified beneficiaries (who are beneficial owners within the meaning of the Beneficial Ownership Act, 2020), or a class of beneficiaries. These persons will be self-evident from a review of the trust's constitution. In the case of a legal arrangement that is not a trust, the beneficial owner means:

- Where the individuals who benefit from the entity or arrangement have been determined, any individual who benefits from the property of the entity or arrangement;

- Where the individuals who benefit from the entity or arrangement have yet to be determined, the class of persons in whose main interest the entity or arrangement is set up or operates;

- Any individual who exercises control over the property of the entity or arrangement.

The Company shall obtain, record and maintain the following details about the trust:

- Full name of Trust;

- Nature and purpose of Trust (e.g. discretionary, testamentary, bare);

- Country of establishment;

- Names of all trustees;

- Names of any beneficial owners;

- Name and address of any protector or controller.

Documentary evidence required to verify legal purpose: Scheme Trust Deed or latest Deed of Appointment, listing all current Trustees.

Additionally, names, addresses and dates of birth and identity verification required for trustees in whose names an investment is registered (i.e. if trustee is a private individual, personal identity and address verification also required).

Names and confirmation of the identity of any other trustees, names and addresses

and confirmation of the identity of any protector or controller, plus names and confirmation of identity of any nominated beneficiaries having an interest in the trust.

5.4.2. Partnership/unincorporated body

Partnerships and unincorporated businesses, although principally operated by individuals, or groups of individuals, are different from private individuals in that there is an underlying business. This business is likely to have a different money laundering or terrorism financing risk profile from that of an individual.

The beneficial owner of a partnership is any individual who ultimately is entitled to or controls (whether the entitlement or control is direct or indirect) share of the capital or profits of the partnership, or voting rights in the partnership, or who otherwise exercise control over the management of the partnership.

In verifying the identity of such customers, primarily have regard to the number of partner/principals. Where these are relatively few, the customer should be treated as a collection of private individuals and identified accordingly.

Where numbers are larger, decide whether to regard the customer as a collection of private individuals, or whether it might be appropriate to be satisfied with evidence of membership of a relevant professional or trade association. In either circumstance, there is likely to be a need to see the partnership deed (or other evidence in the case of sole traders or other unincorporated businesses), to be satisfied that the entity exists, unless an entry in an appropriate national register may be checked.

The Company shall obtain, record and maintain the following details about the partnership:

- Business address;
- Names of all partners/principals who exercise control over the management of the partnership;
- Names of individuals who own or control its capital or profit, or of its voting rights.

Documentary evidence required to verify legal purpose: Partnership deed showing rights and duties of the partners.

Additionally, name, address, date of birth and identity verification is required for partners or owners in whose names investments are registered (i.e. for private individuals, personal identity and address verification is required).

5.4.3. Charities

The Company shall obtain, record and maintain the following details about the trust:

- Nature of body's activities and objects;
- Names of all trustees (or equivalent);
- Names or classes of beneficiaries.

Documentary evidence required to verify legal purpose: charities have their status because of their purposes and can take a number of legal forms. Some may be companies limited by guarantee, or incorporated by Royal Charter or by Act of Parliament; some may take the form of trusts; others may be unincorporated associations.

Additionally, confirmation of the identity of all other officers/trustees (i.e. name, address and dates of birth); this can be achieved by one of the verified partners or proprietors providing an original signed letter on the customer's letterhead, incorporating a listing of relevant persons (i.e. other officers).

5.5. General provisions

If, during the business relationship, the 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.

CDD regarding the private individuals, as well as companies shall be updated and/or amended soon after any changes take place. This refers to change of residential, registered or business address, new identification cards, new passport, additional business information, new business securities/venture, new directors, beneficial owners, expiry of previously submitted documents. For any change of information before the said period the Company requests a letter or document pertaining to the changes being made.

When accepting new customers during the verification process and documents review the Company might apply other requirements and procedures for the customer's identification. Such procedures are to be based on the risk-based approach adopted by the company and subject to variations depending on various factors, including but not limited to the country of residence of the customer, customer's economic profile and others.

The Company shall request the customer to provide a source of funds, source of wealth documents, proof of funds being deposited in a form and manner as the Company finds appropriate and other documents the Company deems necessary to perform all check required under the applicable legislation.

Based on the risk, the Company shall analyze any logical inconsistencies in the information or behavior of its customers. CDD of existing customers shall be updated and/or amended based on the risk level of the customer as follows:

- at least every 6 months for high-risk customers;
- at least every 12 months for normal-risk customer
- at least every 24 month for low-risk customers

The Company shall establish whether the applicant for business relationship is acting on his behalf of on behalf of another person or legal entity. 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 capacity and duties. The Company shall apply similar CDD measures to both the applicant for business relationship and to the person or legal entity he represents or acts on behalf of.

Whether the documents certification is required, the documents shall be certified by one of the following:

- a Judge;
- a Magistrate;
- a notary public;
- a barrister-at-law;
- a Solicitor;
- an attorney-at-law; or
- a Commissioner of Oaths.

6. Risk-based approach

6.1. Application of the risk-based approach

The Company shall apply adequate and appropriate measures, policies, controls and procedures, by developing and implementing a risk-based approach in order to mitigate and effectively manage the risks of money laundering and terrorism financing in a manner to focus its effort in those areas where such risks appear to be comparatively higher.

The adopted risk-based approach that is followed by the Company, and described in the Policy, has the following general characteristics:

- recognizes that the money laundering and terrorism financing threat varies across customers, countries, services and securities;

- allows the Company to differentiate between customers of the Company in a way that matches the risk of their particular business;
- allows the Company to apply its own approach in the formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics;
- helps to produce a more cost-effective system; and
- promotes the prioritization of effort and actions of the Company in response to the likelihood of money laundering or terrorism financing occurring as a result of use of services or products provided by the Company.

The Company shall assess and evaluate the risks it faces, for usage of the services provided for the purpose of money laundering or terrorism financing. The particular circumstances that shall determine the suitable procedures and measures which need to be applied to counter and manage risks including identification, recording and evaluation of risk that the Company faces, presuppose to the finding of the risk posed by the customers' behavior, the way the customer communicate and the risk posed by the services and securities provided by the Company. The Company when assessing the risk of money laundering and terrorism financing shall take into account, among others, the Risk Factor Guidelines and any guidelines/guidance issued by the FATF.

6.2. Identification of risks

The risk-based approach adopted by the Company involves the identification, recording and evaluation of the risks that have to be managed. In the cases where the services and products the Company provides are of the same level, involving relatively few customers or customers with similar characteristics, then the Company shall apply such procedures which are able to focus on those customers who fall outside the 'norm'. The Company shall take the following indicative risk variables into consideration while it determines the risks implicated as well as the categorization of the customers:

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

6.3. Types of risks

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

Money Laundering and Terrorism Financing:

Risks based on the customer's nature	• complexity of ownership structure of legal persons; • 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.
Risks based on the customer's behavior	• customer transactions where there is no apparent legal financial/commercial rationale; • situations where the source of funds and/or source of wealth of the customer or its BOs cannot be easily verified; and • unwillingness of customers to provide information on the BOs of a legal person.
Risks based on the customer's initial communication with the Company	• non face-to-face customers; and • customers introduced by a third party.
Risks based on the Company's services and securities	• services that allow payments to third parties; • large deposits or withdrawals; and • products or transactions which may favor anonymity

Any single match cannot indicate that the customer shall be considered as a high-risk customer. The combination of different matches, background information and customer's activity with the company together contribute to the customer's risk scoring and can result in the customer's risk level to be changed accordingly.

6.4. Measures to mitigate risks

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

- adaption of the CDD and EDD procedures in respect of customers in line with their risk level;
- requiring the quality and extent of required identification data for each type of customer to be of a certain standard (e.g. documents from independent and reliable sources, third party information, documentary evidence);

- obtaining additional data and information from the customers; where this is appropriate for the proper and complete understanding of their activities, source of funds and source of wealth, for the effective management of any increased risk, emanating from the particular business relationship; and

- ongoing monitoring of high-risk customers' transactions and activities, as and when applicable.

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

6.5. Customers categorization

This section describes the criteria for accepting new customers based on their risk categorization as follows:

1. 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 might apply Simplified CDD procedures for low risk customers.

2. Normal risk customers. The Company shall accept customers who are categorized as normal risk customers as long as the general principles are followed. Typically, the normal risk customer is a customer who is neither a low risk customer nor a high risk customer.

3. High risk customers. The Company shall accept customers who are categorized as high-risk customers as long as the general principles are followed. Moreover, the Company shall apply the EDD measures for high risk customers, as well as apply the due diligence and identification procedures for the specific types of high-risk customers mentioned in this Policy, as applicable.

There is also a fourth category of unacceptable customers. The following list predetermines the type of customers or industries who are not acceptable for establishing a business relationship with the Company:

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

- customers included in Sanction Lists;

- shell banks;

- companies with bearer shares or whose BOs cannot be identified;

- correspondent banks.

This section defines the criteria for the categorization of customers based on their risk.

Risk Category	Low risk customers	Normal risk customers	High risk customers
Customer risk factors	• 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; • public administrations or enterprises; • customer that are resident in geographical areas of lower risk.	Any customer who does not fall under the "Low risk customers" or "High risk customers" categories, including customers who are not physically present for identification purposes (non-face-to-face customers).	• the business relationship is conducted in unusual circumstances; • legal persons or arrangements that are personal asset-holding vehicles; • companies that have nominee shareholders; • businesses that are cash-intensive; • the ownership structure of the company appears unusual or excessively complex given the nature of the company's business; • PEPs; • customers convicted for a prescribed offence (and already served their sentence); • unwillingness of customer to provide information on the BOs of a legal person; • trust accounts; • customers' accounts in the name of a third party; • customers who are involved in gambling/ gaming activities; • any other customers that their nature entail a higher risk of money laundering or terrorism financing; and • any other customer determined by the Company itself to be classified as such.
Product, service, transaction or delivery channel risk factors	• financial services or products that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes • products where the risks of money laundering or terrorism financing are managed by other factors.		• products or transactions that might favour anonymity; • payment received from unknown or non-associated third parties; • 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
Geogra-phical risk factors	• the geographical location of the customer's residence; • the geographical location of the customer's business interests and/ or assets.		• customers that are resident in geographical areas of higher risk; • customers from countries which inadequately apply FATF's recommendations; • customers from countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems; • customers from countries identified by credible sources as having significant levels of corruption or other criminal activity; • customers from countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations; • customers from countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.
Risk based on the customer's behavior			• customer transactions where there is no apparent legal financial/commercial rationale • situations where the origin of wealth and/or source of funds cannot be easily verified • unwillingness of customers to provide information upon the Company's request.

6.6. 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 products and services provided by the Company change.

In this respect, it is the duty of the Company to undertake regular reviews of the characteristics of existing customers, new customers, products and services, and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics or circumstances.

7. On-going monitoring

Information collected from (or about) applicants who subsequently become customers, must, as far as reasonably practicable, be kept up to date. Information obtained at customer take-on, or when monitoring for variances against that initial customer profile, is a useful mechanism with which to aid deter and detect potential criminality. The constant monitoring of the customers' accounts and transactions is an imperative element in the implementation of AML and CFT measures.

The Company shall conduct ongoing monitoring of a business relationship by:

- Scrutinising transactions undertaken throughout the relationship to ensure that the transactions are consistent with the reporting entity's knowledge of the customer, the business and risk profile and the source of funds of the customer; and
- Keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up to date.

Once identity is satisfactorily verified, there is usually no need to re-verify identity, unless:

- Subsequent doubts arise as to the veracity or adequacy of evidence previously obtained for the purposes of customer identification;
- The customer changes name (e.g. through marriage or deed-poll for a private individual, or by changing company name, for a legal entity);
- Beneficial ownership or control changes materially to that which was understood and documented at customer onboarding;
- As new/emerging risk dictates.

The Company shall adopt a risk-based approach for the on-going monitoring procedures, which shall be based, inter alia, on the customer's risk categorization,

information obtained about the customer during the onboarding, transactional patterns and volumes of transactions executed with the Company. With regards to the nature and purpose of activity transacted, to ensure that on-going monitoring/risk-assessment of customer transactions is fit-for-purpose, appropriate measures should be taken to maintain up-to-date information about customers, whether on a routine or event driven basis.

7.1. Regular risk assessments and refresh

Ad-hoc risk-based reviews are undertaken on existing relationships at predetermined trigger events, such as:

Out-of-the-ordinary account activity includes:

- An existing customer applying to open a new account or establish a new relationship;
- Change in ownership or control of a customer entity, or change of business, operating or contact address;
- Change of standing data for personal customers, such as, residential or contact address;
- Adverse media reporting about a customer or customer business;
- Transactions with different territories/jurisdictions, particularly higher-risk countries;
- Account inactivity or dormancy for a defined period;
- Other criteria indicating risk of involvement of the customer in money laundering or terrorism financing activities.

A suspicious transaction or suspicious circumstances may arise at any time during a relationship with a customer. The Company shall be on the lookout for any activity which is inconsistent with the customer's expected and legitimate transactions:

- Unusually large deposits – outside the normal trends of the account operation;
- Requests to deposit cash;
- Attempted use of third parties for deposits/withdrawals;
- Payments to/from high risk countries;
- Difficulties in obtaining ID documentation;

- Transactions with no apparent purpose;
- Funding an account but not trading and then withdrawing the funds or when a customer enters into a business relationship with the Company for a single transaction or for a very short period of time only;
- Unusual transactions - activity that is inconsistent or out of the ordinary range of a particular customer's usual trading pattern;
- For corporate accounts, legal and corporate structures, its ownership and control do not make any sense;
- The customer suggesting changes to our procedures in order to avoid providing certain information.

Other things to look out for:

- Sudden, substantial increases in deposits or levels of investment without adequate explanation;
- Large electronic transfers in and out of the account;
- Reactivation of dormant accounts;
- No known source of income or activity inconsistent with a stated occupation;
- Frequent address changes.

The above lists of possible suspicious activities are non-exhaustive and if any activities of a customer seem unusual or if there are any suspicions, it should be reported to the CO.

Transactions undertaken on customer trading accounts will be monitored as part of the Company's risk management strategy. Any transactions which are deemed abnormal or suspicious and have the sign of involvement in the money laundering or terrorism financing activities, reported to the CO.

As part of the regular compliance monitoring initiative, the CO department will undertake a monthly review of compliance with anti-money laundering regulations. A monthly review of KYC documentation will take place. Each month, a random sample of new accounts will be checked to ensure compliance with internal policy and procedures.

Senior management will be informed of the results of this monitoring during the monthly board meetings.

7.2. Suspicious transactions/activities reporting

As a general principle, all Company's Directors, managers and employees shall report

any knowledge or suspicious of money laundering or terrorism financing activity to the CO the. The report shall be formally submitted either in hard copy, or using Company's internal communication systems (including email). Using of any external communication systems for submission of such report is strictly prohibited. Report shall be submitted according to the template of the Internal Suspicion Report for Money Laundering and Terrorist Financing.

The Company, its Directors, managers and employees are not allowed to disclose to the customer or third parties the fact that information on suspicious transaction or activity has been provided to the CO, is being or will be reported to the FIU as well as any measures undertaken.

The CO shall evaluate and check the information received from the internal report, with reference to other available sources of information and the exchanging of information in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained on the report which is submitted to the CO shall be evaluated and results of such evaluation shall be recorded. As a result of such evaluation the CO shall decide whether to report this case further and submit an STR/SAR to the FIU. Reporting any suspicious transaction or activity shall be done by the CO within 48 hours of having information about such suspicion or in any event as soon as it is practicable.

The CO shall maintain the register of all received internal reports, as well as any outcome of the investigation, including, where after throughout evaluation it is determined that there is really a risk or suspicion of money laundering or terrorism financing, details of any STR/SAR submitted to the FIU.

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

- the identity of the account holders;
- the identity of the BOs of the account;
- the identity of the persons authorized to manage the account;
- data of the volume of funds or level of transactions flowing through the account;
- connected accounts;
- in relation to specific transactions:
  - the origin of the funds;
  - the type and amount of the currency involved in the transaction;
  - the form in which the funds were placed or withdrawn, for example cash,

cheques, wire transfers;

- the identity of the person that gave the order for the transaction;
- the destination of the funds;
- the form of instructions and authorization that have been given;
- the type and identifying number of any account involved in the transaction.

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

7.3. Due Diligence on Third Party Relationships

It is essential that firms understand who they working with when establishing business relationships and in doing this firms are expected to:

- Establish and document policies with a clear definition of a 'third party' and the due diligence required when establishing and reviewing third party relationships.
- Have more robust due diligence on third parties which pose the greatest risk of bribery and corruption, including a detailed understanding of the business case for Using them.
- Have a clear understanding of the roles clients, and third party suppliers, such as solicitors undertake in transactions to ensure they are not carrying out higher risk activities.
- Take reasonable steps to verify the information provided by third parties during the due diligence process.
- Use third party forms which ask relevant questions and clearly state which fields are mandatory.
- Have third party account opening forms reviewed and approved by compliance, risk or committees involving these areas.
- Use commercially-available intelligence tools, databases and/or other research techniques such as internet search engines to check third party declarations about connections to public officials, and other parties.

- Routinely inform all parties involved in the transaction about the involvement of third parties being paid commission.
- Ensure current third party due diligence standards are appropriate when business is acquired that is higher risk than existing business.
- Consider the level of bribery and corruption risk posed by a third party when agreeing the level of commission.
- Set commission limits or guidelines which take into account risk factors related to the role of the third party, the country involved and the class of business.
- Pay commission to third parties on a one-off fee basis where their role is pure introduction.
- Take reasonable steps to ensure that bank accounts used by third parties to receive payments are, in fact, controlled by the third party for which the payment is meant. For example, broker firms might wish to see the third party's bank statement or have the third party write them a low value cheque.
- Apply higher or extra levels of approval for high risk third party relationships.
- Regularly review third party relationships to identify the nature and risk profile of third party relationships.
- Maintain accurate central records of approved third parties, the due diligence conducted on the relationship and evidence of periodic reviews.

7.4. Payment Controls

The Company must consider the implications of the AML Act in conjunction with payments, commission and fees it pays by:

- Ensuring adequate due diligence and approval of the payment details before the payments are executed;
- Risk-based approval procedures for payments and a clear understanding of why payments are made;
- Checking payments individually prior to approval, to ensure consistency with the business case for that account;
- Regular and thorough monitoring of payments to check, for example, whether a payment is unusual in the context of previous similar payments;
- Not allowing any payments from third parties to be accepted on the customer's account and not send any funds from the customer's account to

any third party;

- Ensuring the clear system is implemented by which withdrawal transactions shall be processed to the customer to the same account where the deposit came from, on a pro rata basis commensurate to the size of each initial deposit, on the First In First Out basis, while any excess can be transferred to the account of the customer's preference open in his name;

- Clear limits on staff expenditure, which are fully documented, communicated to staff and enforced;

7.5. Staff Recruitment and Vetting

When new or existing staffs are appointed to new roles the Company has an obligation to:

- Vet staff on a risk-based approach, taking into account financial crime risk;

- Enhance vetting – including checks of credit records, criminal records, financial sanctions lists, commercially available intelligence databases– for staff in roles with higher bribery and corruption risk;

- Apply risk-based approach to dealing with adverse information raised by vetting checks, taking into account its seriousness and relevance in the context of the individual's role or proposed role;

- Ensure that where employment agencies are used to recruit staff in higher risk positions, having a clear understanding of the checks they carry out on prospective staff;

- Conduct periodic checks to ensure that agencies are complying with agreed vetting standards;

- Apply a formal process for identifying changes in existing employees' financial soundness which might make them more vulnerable to becoming involved in or committing corrupt practices.

7.6. Training and Awareness

The Company shall provide the necessary training to its Directors, managers and employees, and CO in particular. The Company disseminates to the staff the new procedures and guidelines needed in combating money laundering and terrorism financing.

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

The Company must ensure that it:

- Provides good quality, standard training on AML, CFT, anti-bribery and corruption for all staff;
- Has additional AML, CFT, anti-bribery and corruption training for staff in higher risk positions;
- Ensure staffs responsible for training others have adequate training themselves;
- Ensure training covers practical examples of risk and how to comply with policies;
- Test staff understanding and using the results to assess individual training needs and the overall quality of the training;
- The staff records setting out what training was completed and when;
- Provide refresher training and ensuring it is kept up-to-date.

8. Record keeping

8.1. Adequate records

The Company, having considered the regulations, insist appropriate records concerning customer identification and transactions must be maintained, as evidence of work undertaken in complying with any legal and regulatory obligations, as well as for use as evidence in any investigation conducted by a law enforcement agency or regulatory body.

Reasonable care must be taken to make and keep adequate records appropriate to the scale, nature and complexity of business undertaken with customers, covering:

- Customer information;
- Transactions;
- Internal reports and external STR/SARs;
- Information not acted upon;
- CO's annual (and other) reports;
- Training (and information about the effectiveness of training);
- Compliance monitoring information.

8.2. Customer information

With regard to customer information, records to be retained are:

- A copy of, or the references to, the evidence of customer identity obtained when establishing (or updating) details held about a customer; monitoring the business relationship; or when performing enhanced due diligence (‘customer records’);

- The supporting records (consisting of the original documents or appropriate copies) in respect of business relationships or occasional transactions which are the subject of customer due diligence measures or on-going monitoring (‘customer supporting records’).

The following document retention periods will be followed:

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

- 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.