Performance Corp.

New Era Broker

AML /CFT Manual

June2026
V: 1.1.

Table of Contents

1. Introduction

This Anti-Money Laundering and Counter-Terrorist Financing Manual (the 'AML Manual' and/or Manual) sets out the policies, procedures, and controls adopted by **Performance Corp**., a Saint Lucia–based investment services provider offering over-the-counter (the 'OTC') trading in Contracts for Difference (the 'CFDs'). The objective of this Manual is to prevent the misuse of the Company's services for money laundering, terrorist financing, or related financial crimes. This Manual does not substitute the principles, laws, or other code of conduct applicable in St. Lucia or any other applicable jurisdictions but only complements and enhances them.

Good compliance is good business and is also vital to sustaining in business. Any company that does not believe in this principle will not remain in business. The preservation of the good name and reputation built along time requires the adoption of policies to prevent situations in which there may be conflicts of interest among clients, the Company and/or its employees. The Company by the very nature of its business deals with confidential privileged information; and hence there is a greater possibility that conflict of interest may occur.

2. Scope

All officers and employees are expected to have read and understood the contents of this Manual in so far as it is applicable to him/her and shall abide by these principles and any deviation from them will not be tolerated. The Company's staff must also refer and keep themselves up to date with the relevant rules and regulations applicable.

3. Definitions

(a) Applicant for business" means a person, who seeks to form a business relationship, or carry out an occasional with a reporting person.

(b) "customer" means a natural person or a legal person or a legal arrangement for whom a transaction or account is arranged, opened or undertaken and includes:

- i. a signatory to a transaction or account;
- ii. any person to whom an account or rights or obligations under a transaction have been assigned or transferred;
- iii. any person who is authorized to conduct a transaction or control an account;
- iv. any person who attempts to take any action referred to above; and
- v. an applicant for business.

(c) "suspicious transaction" means a transaction which:

- i. gives rise to a reasonable suspicion that it may involve:
- ii. the laundering of money or the proceeds of any crime; or
- iii. funds linked or related to, or to be used for, the financing of terrorism or proliferation financing or, any other activities or transaction related to terrorism as specified in the Prevention of Terrorism Act or under any other enactment, whether the funds represent the proceeds of a crime;

iv. is made in circumstances of unusual or unjustified complexity;
v. appears to have no economic justification or lawful objective;
vi. is made by or on behalf of a person whose identity has not been established to the satisfaction of the person with whom the transaction is made; or
vii. gives rise to suspicion for any other reason.

The following are some indicators of potentially suspicious activity, and should arouse skepticism as the source of funds for the transaction:

(a) any activity that casts doubt over the true identity of an applicant for business or principals thereof;
(b) establishment of companies having no obvious commercial purpose;
(c) unusually linked transactions;
(d) unwillingness to disclose source of funds;
(e) complex structures with no obvious commercial purpose;
(f) activities that appear to be inconsistent with the KYC information and profile of the client;
(g) fund transfer to or from accounts in Financial Action Task Force ("FATF") non co- operative countries and territories or countries that are known to be associated with drug trafficking or other serious crimes.

4. General Rules of Conduct

In order to fulfil this role, the Company needs to maintain the confidence of its clients, shareholders and employees, and other stakeholders by acting with professionalism and integrity as well as behaving with prudence and skill.

The Company, therefore, attaches paramount importance to upholding its reputation. It is the responsibility of everyone in the Company to maintain its standing for high ethical standards of conduct. This requires constant vigilance and application.

The General rules described in this statement do not merely reflect laws and regulations; they are also based upon values of integrity, entrepreneurship, professionalism, responsiveness and teamwork.

These General rules apply to the whole of the Company and all employees who are required to act in accordance with both the letter and spirit of these General rules. It is the responsibility of all those in authority in the Company to ensure that these General rules are fully communicated to all employees and that they are strictly observed.

All staff members are required to comply with all applicable laws, rules and regulations, whether or not specifically addressed in this Manual. Whenever a difficulty arises over the application or meaning of a particular rule or regulation, recourse should always be made to the compliance officer of the Company (the "Compliance Officer" and /or the "CO") whose functions are more fully particularized below.

Staff must co-operate fully with any supervision team visiting the Company, including, but not limited to, answering all questions posed by the inspectors, truthfully and without constraint. Any staff member

receiving a request for assistance, evidence or any other information from outside regulatory bodies should immediately enlist the assistance of the Compliance Officer.

Staff members should not make direct contact with any supervision team but should address questions or concerns about any compliance or regulatory issue to the nominated Compliance Officer.

5. Governance and Responsibility

5.1. Board of Directors

5.1.1. General Responsibilities

The responsibilities of the Board in relation to the prevention and suppression of Money Laundering and Terrorist Financing include the following:

(a) to have direct and continuous overview of the money laundering and terrorist financing issues;
(b) to determine, record and approve the general policy principles of the Company in relation to the prevention and suppression of Money Laundering and Terrorist Financing and communicate them to the CO;
(c) to appoint a senior official that possesses the skills, knowledge and expertise relevant to financial and other activities depending on the situation, who shall act as the CO and, where is necessary, assistant COs and determine their duties and responsibilities, which are recorded in this Manual. Only persons who shall possess the relevant certificate(s) of professional competence shall be appointed as CO and assistant COs;
(d) to appoint, in case of the absence of the CO, an Alternate CO (hereinafter "Alternate CO"), if deemed necessary;
(e) to ensure that the Alternate CO possesses the relevant skills, knowledge and expertise for carrying out the duties of the CO as described in this Manual;
(f) to approve the Manual and any updated version of it;
(g) to ensure that the CO, alternate CO and their assistants, if any, and any other person who has been assigned with the duty of implementing the procedures for the prevention and suppression of Money Laundering and Terrorist Financing (i.e. personnel of the Administration/Back-Office Department), have complete and timely access to all data and information concerning Clients' identity, transactions' documents (as and where applicable) and other relevant files and information maintained by the Company so as to be fully facilitated in the effective execution of their duties, as included herein;
(h) to ensure that all employees are aware of the person who has been assigned the duties of the CO and Alternate CO, as well as their assistants (if any), to whom they report any information concerning transactions and activities for which they have knowledge or suspicion that might be related to Money Laundering and Terrorist Financing;
(i) to establish a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the CO or Alternate CO, either directly or through his assistants, if any, and notifies accordingly the CO or Alternate CO for its explicit prescription in the Manual;

(j) to ensure that the CO, the Alternate CO, the assistants COs, if any, and the Administration/Back-Office Department have sufficient resources, including competent staff and technological equipment, for the effective discharge of their duties;
(k) to meet and decide the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected.
(l) to implement adequate and appropriate systems and processes to detect, prevent and deter money laundering arising from serious tax offences;
(m) to ensure that the Company's officials do not knowingly aid or abet clients in committing tax offences;
(n) to approve the mandatory annual training programme prepared by the CO;
(o) to ensure that they receive adequate management information on the implementation of the Company's training programme;

5.1.2. AML/ CFT Responsibilities

From an AML/CFT perspective, the Board needs to:

(a) have broad oversight on compliance with the provisions of this Policy and providing guidelines regarding the management of AML/CFT compliance risks on a risk-based approach;
(b) ensure that systems and controls are appropriately designed, documented and implemented, and are effectively operated to reduce the risk of the business being used in connection with AML/CFT;
(c) ensure that the AML/CFT framework devised for the Company is reviewed and kept relevant and up to date;
(d) determine the nature and extent of compliance reviews commensurate with the risk assessments, size and nature of business of the Company;
(e) appoint all relevant officers required under the relevant AML/CFT regulations including a compliance officerand apportion responsibilities for combatting AML/CFT;
(f) be responsible for reviewing and making decisions, based on reports received on AML/CFT matters;
(g) devise screening procedures to ensure high standards when hiring employees;
(h) implement an ongoing training programme for its directors, officers and employees, as applicable, to maintain awareness of the Relevant Laws;
(i) maintain records in line with the regulatory requirements, and
(j) appoint an independent audit function to test the policies, procedures and controls of the Company regarding AML/CFT.

5.2. Compliance Officer

The Compliance Officer is the officer primarily responsible for overseeing and managing compliance issues within the Company. They have a duty to report to the board of directors of the Company (the "Board") or any other person appointed by the Board on the progress of implementation and review of the Company's policies and procedures and staff training. In the event of the Compliance Officer's absence from the Company, one of the directors of the Company will act as the alternate compliance officer and will assume the responsibilities of the Compliance Officer.

The main responsibilities of the Compliance Officer are, inter alia, but not limited to, the following:

(a) the effective implementation of the provisions contained in this Manual;
(b) the effective implementation of the applicable laws and regulations;
(c) to brief the directors of the Company on matters relating to compliance;
(d) ensure that the staff of the Company are trained on a regular and continuous basis to ensure that they understand this Manual and the laws relating to Anti Money Laundering and Prevention of Corruption;
(e) to advise directors on the impact of likely changes in legislation and procedures relating to compliance matters;
(f) to meet the reporting requirements relating to statutory, regulatory and supervisory matters;
(g) to conduct review of files to generally ensure that all compliance requirements are met;
(h) to determine whether any existing business relationships exist with persons or groups with known or suspected links to terrorist activity;
(i) to conduct similar reviews when names are added to any existing lists of known or suspected terrorists;
(j) on a pro-active basis, to identify and assess the compliance risks associated with the company activities, including in relation to the development of new products and business practices, the proposed establishment of new business or customer relationships, or material changes in the nature of such relationships;
(k) to establish written guidance to staff on the appropriate implementation of the laws, rules and standards through policies and procedures and, when necessary, formulating proposals for amendments;
(l) to monitor compliance with policy by performing regular and comprehensive compliance risk assessment and testing, and reporting on a regular basis to Senior Management, and if necessary, the Board or a committee of the Board, on compliance matters, the reports should refer to the compliance risk assessment and testing which has taken place during the reporting period, any identified breaches and/or deficiencies, and the corrective action taken. The reports should also contain information about compliance function and other staff;
(m) to educate staff with respect to compliance with the applicable laws, rules and standards, and acting as a contact point within the Company and other staff; and
(n) to liaise with relevant external bodies, including regulators, and external legal counsel.

The Compliance Officer shall also:

(a) analyse regularly the business and compliance risks;
(b) review the compliance strategy;
(c) reassess the compliance standards in place and analyse how current standards are being met;
(d) review training and competence arrangements;
(e) broaden and deepen relationships with the regulator;
(f) review Senior Management responsibilities;
(g) review the structure and reporting lines of the Compliance Department;
(h) consider the adequacy of compliance resources;
(i) assess how well compliance issues are being communicated and acted upon;
(j) build compliance into the Company's Day to day management decision processes;

(k) build compliance into the governance of the Company;
(l) perform compliance monitoring subject to an approved plan;
(m) perform compliance risk management subject to an approved yearly plan which is reportable every quarter; and
(n) provide regular communication and training to all staff on matters arising from the monitoring and risk management plans.

6. Operating Principles

6.1. Personal Conduct

The Company expects the highest levels of personal conduct by all its employees, whatever their position. It is acknowledged that all effective business relationships depend upon honesty, integrity and fairness.

While it is recognized that limited corporate hospitality is given and received as part of building normal business relationships, employees should avoid accepting hospitality or gifts that might appear to place them under an obligation.

Bribery of any form is unacceptable. No undeclared offers or payments will be accepted or solicited by employees, or made by employees to third parties, and employees are required to avoid any contacts that might lead to, or suggest, a conflict of interest between their personal activities and the business of the Company.

The Company expects all its employees to respect the rule of law and abide by appropriate regulations. Furthermore, all employees are expected to avoid doing business with any individual, company or institution if that business is connected with activities which are illegal or which could be regarded as unethical.

6.2. Co-operation with Auditors and Authorities

The Company will respond honestly and candidly and disclose information fully, accurately when dealing with the Company's auditors, authorities and attorneys.

6.3. Operation

The Company wishes to have an unimpeachable reputation for integrity; therefore, it is essential that the Company can be judged by its actions. As these business principles make clear, this depends upon the conduct of every individual in the Company.

All employees must be familiar with these standards and apply them consistently and rigorously in business activities each day. It is important that the conduct of a few, whether through misplaced zeal or short-term expediency, should not damage the reputation of the many in the Company.

All employees are responsible for the application of the principles across the Company and must lead by example.

The most effective assurance mechanism is constant vigilance by all employees, always, to ensure that the Company is clearly seen to act in keeping with the commitment to maintain high ethical standards.

6.4. Fair Dealing

The Company will seek competitive advantage through superior and honest performance, never through unethical or illegal business practices. It will endeavor to deal fairly and honestly with:

(a) the Company's clients;
(b) suppliers;
(c) competitors; and
(d) vendors.

The Company will not take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts or any unfair dealing.

6.5. Business Risk Assessment

To ensure sound and prudent governance and management of the Company, its operation as well as the relationship with Clients, the Company shall identify, assess, understand and monitor money laundering and terrorism financing risks.

While performing business, Management, Compliance and Risk Management should all work together on performing the Business Risk Assessment. Primarily, responsibility for the quality and execution of the risk analyses lies with the first line of defence. This is the business, as risks manifest themselves first there. The role of Compliance is process monitoring, facilitating and testing. Other functions or departments such as Audit can also provide the necessary input. The ultimate responsibility for the Business Risk Assessment lies with the Board of Directors.

The 6 key areas which shall be considered when undertaking the business risk assessment amongst other risk factors are:

(a) the nature, scale and complexity of the financial institution's activities;
(b) the products and services provided by the financial institution's;
(c) the persons to whom and the manner in which the products and services are provided;
(d) the nature, scale, complexity and location of the customer's activities;
(e) reliance on third parties for elements of the customer due diligence process; and
(f) technological developments.

Furthermore, the Company undertakes to update the Business Risk Assessment on, at least, an annual basis or at shorter intervals in case of need.

7. AML /CFT Key Points

7.1. What are Money Laundering and Terrorist Financing

7.1.1. Money Laundering

Money laundering is a process through which illegally gained proceeds are brought back into the economy as legitimate income.

The Financial Action Task Force describes Money laundering as "the processing of criminal proceeds in order to disguise their illegal origin".

Examples of crimes through which dirty money may be obtained include kidnapping, drug trafficking, bribery/corruption, forgery, prostitution, smuggling, extortion, and tax evasion.

Money Laundering is usually based on the following objectives:

(a) To conceal the origin and true ownership of criminal proceeds
(b) To maintain control over the proceeds
(c) To enjoy profits of crime in the guise of legitimate business

There are three recognized stages of the Money Laundering process:

(a) PLACEMENT
This is the stage at which illicit funds are separated from their illegal source. Placement involves the initial injection of the illegal funds into the financial system or carrying of cash across borders.

(b) LAYERING
This is the stage at which the launderer engages in a series of conversions or movements of the funds to distance them from their source. Money laundering requires the creation of multiple layers of transactions that further separate the funds from their illegal source. The purpose of this stage is to make it more difficult to trace these funds to their illegal source.

(c) INTEGRATION
This is the stage at which the funds re-enter the legitimate economy. The funds now appear as clean income.

7.1.2. Terrorist Financing

Terrorist financing is the provision or collection of funds by any means, directly or indirectly, with the intention that they should be used, in full or in part, in order to carry out terrorist offences.

Acts of terror and the terrorist groups that commit them require funding in much the same way that criminal organizations require money to further their criminal activities.

7.1.3. Proliferation Financing

Proliferation of weapons of mass destruction (the "WMDs") can be in many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programs involving nuclear, biological or chemical weapons, and their delivery systems (such as long-range missiles).

Proliferation of WMD financing is an important element and, as with international criminal networks, proliferation support networks may use the international financial system to carry out transactions and business deals. Unscrupulous persons may also take advantage of the potential profits to be made by facilitating the movements of sensitive materials, goods, technology and expertise, providing seemingly legitimate front organizations or acting as representatives or middlemen.

8. Client Acceptance Policy

The Client Acceptance Policy (the "CAP"), following the principles and guidelines described in this Manual, defines the criteria for accepting new Clients and defines the Client categorisation criteria which shall be followed by the Company and especially by the employees which shall be involved in the Client Account Opening process.

The CO shall be responsible for applying all the provisions of the CAP. In this respect, the Head of the Administration/Back Office Department shall also be assisting the CO with the implementation of the CAP, as applicable.

The General Principles of the CAP are the following:

(a) the Company shall classify Clients into various risk categories and based on the risk assesment decide on the acceptance criteria for each category of Client
(b) where the Client is a prospective Client, an account must be opened only after the relevant pre-account opening due diligence and identification measures and procedures have been conducted
(c) all documents and data relevant for the Client Account Opening process must be collected before the establishment of a business relationship with a new Client
(d) by way of derogation of point (c) above, the verification of the identity of a new Client may be completed during the establishment of the business relationship
(e) no account shall be opened in anonymous or fictitious names(s)
(f) no account shall be opened unless the prospective Client is approved by at least one of the following:
    a. The Compliance Office
    b. Back Office Head
    c. Senior Manager

8.1. Client Onboarding

The steps involving client onboarding shall be as follows:

(a) following the introductory meeting/first contact with the client, a client profile is established. This includes determining the risk tolerance, return objectives, assessing client's preferences;

(b) customer due diligence (the "CCD") documents are then requested from the client to determine whether they can be onboarded from a CDD perspective.
(c) the company has adopted a system of risk profiling whereby every client is categorized according to the risks that it represents. The due diligence documents to be requested on each type of client is listed in this Manual;
(d) when conducting CDD verification on a legal person, verification is done at a minimum on the following:
    a. promoters;
    b. beneficial owners and ultimate beneficial owners;
    c. officers;
    d. controllers; and
    e. company directors;
(e) The Company applies CDD measures on all clients. However, in certain circumstances where it is deemed that the risk of money laundering is at a minimum, the company will apply simplified due diligence (the "SDD") measures. In case the company will apply these reduced DD measures it shall maintain evidence justifying the application of reduced measures and maintain a record;
(f) enhanced due diligence (the "EDD") measures shall apply to high-risk business relationship. This type of due diligence will be performed when the Company assesses a certain situation to be of a high-risk nature. Factors that may be considered are the nature of the customer, the business relationship, its location, or any other specificity of the business relationship. Additional steps include requests for additional due diligence documents and screening of clients;
(g) at the time of client onboarding, the source of funds of the client (UBO) is also established;
(h) if all due diligence documents are in order, the client is approved by the Company; and, in case of high-risk clients, explicit approval by the CO and Managing Director shall apply;
(i) should the client not meet the CDD verification, the client is declined;
(j) a discretionary or non-discretionary advisory agreement is then entered between the Company and the client. The agreement will lay out the powers delegated by the client to the Company and its agents in respect of the management of the client's portfolio;
(k) once the relationship has been established with the client, the Company will conduct a regular check regarding the relevance of due diligence measures being applied. The ongoing monitoring exercise of the Company consists in the following:
(l) risk profiling review based on events and transactions; and
(m) questioning complex arrangement of the customers and obtaining evidence of same; and
(n) holding appropriate documentation such as: Investment proof and due diligence documents in case of investments, Agreements, Due diligence documentation on parties with which it interacts in line with its KYC requirements.

The potential client has to complete and sign the Account Opening Form.

Information the Client must provide through Account Opening Form:

- Full legal name
- E-mail

- Country of residence
- Phone number
- Information required by the Client Onboarding Questionnaire as attached in Annex 2 to this Manual

Once the above information is provided, the Company may establish a trading account for the Client and grant them access to the Platform via issuance of the login credentials, however, in order to commence trading activities, the Client must, before depositing any funds into their trading account, also submit the KYC documents for verification in accordance with their respective risk category, and as minimum:

- Proof of Identity -a copy of a valid government-issued identification document (e.g., Passport, National ID);
- Proof of Address /Residence -a copy of a utility bill issued in the name of the Client and indicative of their address, which is no older than 3-months;
- Corporate Certificates (in case of legal persons) -including, but not limited to, the following: Certificate of Incorporation, Certificate of Shareholders /UBOs, Certificate of Directors and Secretary, Certificate of Registered Address, Certificate of Good Standing as well as details and KYC of the Beneficial Owner(s).

The above may be further extended, depending on the risk classification of the Client, by additional documents, which may include, inter alia:

- Source of Funds Declaration and supporting evidence;
- Clean Criminal Record;
- CVs and professional certificates;
- Additional POI and /or POR;
- Any other evidence or supporting document deemed necessary in the context of the business relationship.

Once the above is done, the Compliance team must fill in the Risk Profiling Checklist. The KYC document need to be verified and approved by Compliance and where grounds exist, e.g., high -risk business relationship, also by the CEO/Managing Director.

The Company must undertake CDD measures and be satisfied with the results obtained prior to transacting with any client.

The Company may stop at any time the onboarding of clients based on non-business- related criteria such as ML/TF and related risks. The decision to reject such clients need not be due to high-risk criteria only but may be due to the behaviour of the client.

Once the onboarding process has been completed, the Company may reject/exit a client due to the following reasons:

(a) residual risk is too high following adverse hits triggered on the client;
(b) onboarding a client may create a conflict of interest with the organisation;
(c) there are on-going criminal investigations on the client; or

(d) live ML/TF risks.

The decision to reject or off-board a client should be taken together with the CO and the CEO/Managing Director and recorded by email. Any such decision should also be recorded in a log.

In case of suspicious transactions or a need to file an Suspicious Transaction Report, the CO shall consider same.

8.2. Client Due Diligence Measures

As a matter of internal policy, the full range of CDD measures should be applicable using a risk- based approach as provided for in our Risk Profiling Checklist. CDD measures include:

(a) identifying and verifying the identity of the applicant using reliable, independent source documents, data or information;
(b) identifying and verifying the identity of the beneficial owner (ultimate owner), such that the Company is satisfied that it knows who the beneficial owner is. Note: the Company regards the beneficial owner as the natural person(s) who ultimately own(s) or control(s) a client and/or the person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement;
(c) obtaining information on the purpose and intended nature of the business relationship; and
(d) conducting ongoing due diligence on the business relationship and scrutiny of transactions throughout the course of the business relationship with eligible introducer's knowledge of the client and his business and risk profile (including the source of funds).

8.2.1. Identification and Verification of Natural Persons

A. Identification

The Company must collect relevant identification data on a natural person, which includes:

(a) name (including any former names, any other names used and other aliases);
(b) current residential address;
(c) date and place of birth; and
(d) nationality.

B. Verification

(a) Verification of the identity of the natural person
The following types of identity documentation can be relied upon:
    a. national identity cards; and
    b. current valid passports

(b) Verification of the address of the natural person
    a. The following identity documentation can be relied upon to verify the address of the applicant if he/she is a natural person:
    b. a recent utility bill issued not later than 3 months;

c. a recent bank or credit card statement dated; or
d. a recent bank reference.

(c) Alternatively, verification may be achieved by:
a. obtaining a reference from a professional person who knows the natural person. The reference must include the permanent residential address of the individual;
b. checking a current register of electors;
c. utilizing an address verification service; or
d. visit the individual at his/her current residential address.

8.2.2. Identification and Verification of Legal Persons

Legal people include bodies corporate, partnerships, associations or any other body of persons other than legal arrangements.

A. VERIFICATION OF THE EXISTENCE OF A LEGAL PERSON AND IDENTIFYING THE PRINCIPALS THEREOF

Where an applicant is a legal person, the Company must –

a. take reasonable measures to understand the ownership and control structure of the applicant;
b. verify and establish the existence of the legal person; and
c. determine the identity of the principals of the legal person.

For avoidance of doubt, in the case of a legal person, principals of applicants for business include the following:

a. promoters;
b. beneficial owners and ultimate beneficial owners;
c. officers
d. controller; and
e. company directors.

The Company must:

a. identify and verify the identity of the legal person, including name, incorporation number, date and country of incorporation or registration;
b. identify and verify any registered office address and principal place of business (where different from the registered office);
c. verify the legal status of the legal person; and
d. identify and verify the identity of underlying principal (including beneficial owners, controllers, directors or equivalent) with ultimate effective control over the capital or assets of the legal person; and
e. verify that any person who purports to act on behalf of the legal person is duly authorized and identify that person.

Where the underlying principals are not natural persons, the Company should 'drill down' to establish the identity of the natural persons ultimately owning or controlling the business.

B. PRIVATE COMPANIES

This would involve:

a. obtaining an original or appropriately certified copy of the certificate of incorporation or registration;
b. checking with the relevant companies' registry that the company continues to exist;
c. reviewing a copy of the latest report and accounts if available (audited, where possible);
d. obtaining details of the registered office and place of business; and
e. verifying the identity of the principals of the company as above.

C. LEGAL ARRANGEMENTS

Trusts do not have separate legal personality and therefore form business relationships through their business. It is the trustee of the trust who will enter into a business relationship on behalf of the trust and should be considered along with the trust as the client.

D. VERIFICATION OF THE EXISTENCE OF A LEGAL ARRANGEMENT AND IDENTIFYING THE PRINCIPALS THEREOF

Where an applicant is a legal arrangement, the Company:

a. take reasonable measures to understand the ownership and control structure of the applicant;
b. verify and establish the existence of the legal arrangement; and
c. determine the identity of the principals of the legal arrangement.

For the avoidance of doubt, in the case of a legal arrangement, principals of applicants for business include the following:

a. settlors or Contributors of capital (whether named or otherwise);
b. trustees;
c. beneficiaries;
d. protectors; and
e. enforcers

The Company must:

a. verify the legal status of the legal arrangement;
b. identify and verify the identity of the principals of the applicant, that is, those natural persons with a controlling interest and those who comprise the mind and management of the legal arrangement; and

c. obtain information concerning the name of trustee(s), its legal form, address and provisions binding the legal arrangement.

In relation to a trust, the above requirements can be achieved by:

a. obtaining an original or appropriately certified copy of the trust deed or pertinent extracts thereof;
b. where the trust is registered – checking with the relevant registry to ensure that the trust does exist; and
c. obtaining details of the registered office and place of business of the trustee; ▪ Verifying the identity of the principals of the trustee as above.

8.2.3. Timing of Verification

The Company must take all reasonable measures to complete all CDD measures for all applicants prior to transacting with the Client.

The CDD measures must in any event be satisfactorily completed, such that:

(a) it occurs as soon as reasonably practicable;
(b) it is essential not to interrupt the normal conduct of business; and
(c) the money laundering risks are effectively managed.

The Company has appropriate and effective policies, procedures and controls in place, to manage the risk, which include:

(a) establishing that this is not a high-risk relationship;
(b) monitoring by senior management of these business relationships to ensure that the verification of identity is completed as soon as reasonably practicable;
(c) ensuring funds received are not passed on to third parties; and
(d) monitoring large transactions.

In the event that satisfactory CDD documentation has not been obtained, the Company has procedures in place to disengage from or terminate such business relationships. The Company should consider the potential risks inherent in engaging in any form of relationship with any applicant prior to satisfactorily completing CDD measures.

If the Company is unable to:

(a) establish and verify the identity of a customer or other relevant person;
(b) obtain information to understand the nature and intended purpose of the business relationship and source of funds; or
(c) conduct on-going due diligence,

the Company:

(a) may not establish a business relationship or conclude a single transaction with a customer; and
(b) may not conclude a transaction in the course of a business relationship, or perform any act to give effect to a single transaction;
(c) and must terminate an existing business relationship with a customer.

The Company shall also consider submitting an STR if the circumstances which prevent the Company from conducting customer due diligence are suspicious or unusual.

8.2.4. Screening

The Company will screen clients and their related persons at each transaction, at the time of regular review and onboarding. The appropriate checklist will have adequate sections to confirm that screening has been carried out and the results/recommendations thereof.

The screening system used by the Compamy includes a manual screening for all persons, i.e. all persons which are deemed to be controllers or related persons of the client, to be selected on the system for ongoing screening.

A designated officer will perform the relevant screening check and generate a report of the same. In cases where there is a true hit, the Compliance will thereafter review the hit and escalate to the CEO/Managing Director as appropriate for further information. If the hit is not cleared, the CEO/Managing Director will contact the client for further information subject to guidance from Compliance.

The Company may perform more regular review of a client subject to the true hit. The client subject to the true hit will be re-rated as high risk. Transaction monitoring will be more robust and intrusive for high-risk clients.

If following a client review and screening, the client becomes high risk, this will be reported to the Compliance Officer. In any other case, Compliance will perform enhanced due diligence which is appropriate to the risk rating and based on the business as well as transactions of the client.

It is apposite that all such results from reviews and actions undertaken following screening reports must be documented, adequately recorded and kept on file for 7 years.

Any person who holds, controls or has in his custody or possession any funds or other assets of a listed party must, notify, withing 24 hours, the competent authorities in writing of:

(a) details of the funds or other assets against which action was taken in accordance with the prohibition to deal with the funds or other assets of a Listed Party;
(b) the name and address of the Listed Party;
(c) details of any attempted transaction involving the funds or other assets, including:
    a. the name and address of the sender;
    b. the name and address of the intended recipient;
    c. the purpose of the attempted transaction;
    d. the origin of the funds or other assets; and
    e. where the funds or other assets were intended to be sent.

Any person who fails to comply with the above shall commit an offence and shall, on conviction, be liable to a statutory fine and /or to imprisonment.

8.2.5. Sanctions

The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (the "Act") enables the Governments to implement targeted sanctions.

The published lists of applicable sanctions which must at all times be observed by the Company. For this reason the Company utilizes WorldCheck software, which screens the Client against the following:

- **Major Global Sanctions Lists,** such as**:**
    - **OFAC (Office of Foreign Assets Control):** US sanctions list, including Specially Designated Nationals (SDN).
    - **UN Security Council:** Sanctions lists related to terrorism, weapon proliferation, and human rights abuses.
    - **EU Consolidated List:** Financial sanctions from the European Union.
    - **HMT (HM Treasury):** UK sanctions list.
    - **DFAT (Department of Foreign Affairs and Trade):** Australia sanctions list.
    - **Global Affairs Canada:** Canadian sanctions.
- **Specific Jurisdictional & Specialized Lists,** such as**:**
    - **Interpol:** Wanted persons.
    - **PEP Databases:** Politically Exposed Persons (PEPs), their relatives, and close associates.
    - **Regional Watchlists:** Various national, regional, and sector-specific enforcement lists (e.g., Turkey Public Procurement, UAE warnings).

The procedure for screening against sanctions lists:

Step 1: Screening of the lists received to test the screening software to confirm whether hits are captured on the names appearing on the sanctions list.

Step 2: Compliance team tally the lists with the client database. If there is no match, go to step 3. In the contrary, proceed to step 4.

Step 3: Findings are filed.

Step 4: If the name captured relates to one of the clients, the Compliance Officer will make an internal report.

Step 5: The CO will analyse the case and validate the report to the competent authorities.

The Company has adopted the policy of not dealing, directly or indirectly, with any sanctioned/designated list persons or country whether or not the dealing may be legitimate or not and whatever the size of the business.

The Compliance Officer screens client's database against sanctions lists issued by the above bodies as well as the sanction list on the internal screening tool of the Company at take-on and on a regular basis via the ongoing monitoring and as for transactions. It is important that any risk of dealing with sanctioned countries or persons by clients is duly escalated to the CEO/Managing Director and CO.

Each time the Company receives communique of any additional or removal, the process is as follows:

(a) the Compliance Officer screens the lists against our client database;
(b) the list is also screened by Compliance to ensure the screening tool captures these hits;
(c) a nil report is made on the same or next working day and recorder

Compliance will be responsible to escalate all matters relating to sanctioned persons and countries to management. In addition, Compliance shall be responsible to report to the appropriate authorities and the National Sanctions Secretariat in the appropriate format all cases when there are transactions in accordance to the UN Sanctions Act (or such appropriate guidance) immediately, i.e. within 24 hours.

The Company has the obligation to comply with the following:

(a) prohibition to deal with funds or other assets of a listed party under section 23 of the Act; and
(b) prohibition to make funds or other assets available to a listed party under section 24 of the Act.

8.2.6. Adverse Media

The Company has the duty and obligation to ensure the sound conduct of business and have to establish standards in order to preserve and maintain the good repute of St. Lucia as an international financial centre.

When the Company comes across any adverse hits on one of its clients, it shall inform the Commission of the adversely commented press report, and/or public criticism, through prompt submission of a compliance report signed by the director.

The procedure for adverse media screening:

Step 1: Screening of the lists received to test the screening software to confirm whether adverse media hits are captured on the names.

Step 2: Compliance team tally the lists with the client database. If there is no match, go to step 3. In the contrary, proceed to step 4.

Step 3: Findings are filed.

Step 4: If the name captured relates to one of the clients, the Compliance Officer will make an internal report.

Step 5: The CO will analyze the case and validate the report to the Senior Management.

8.2.7. Risk Profiling

After the collection of the CDD documentation, the Company must make an initial assessment of the risk to which the business relationship will expose it and evaluate the client accordingly. In this exercise, the Company take into consideration a number of factors, including but not limited to the following:

(a) the nature and type of client;
(b) the geographical location of the client's residence ;
(c) the geographical location of the client's business interests and/or assets;
(d) the nature and value of the assets concerned in the relationship;
(e) the client's source of funds and where necessary the source of wealth; and
(f) the role of any introducer and the introducer's regulated or professional status

The Company must routinely consider the risks that all relationships pose to them and the manner in which those risks can be limited. To do so, the Company must be able to demonstrate the effective use of documented CDD information. If the Company does not 'know a client', it will not be in a position to recognize and manage the risks inherent to the relationship.

On-going monitoring of client transactions and on-going reviews are fundamental components of an appropriate risk-based assessment.

In terms of risk weightage, the Company should ensure that there is no undue influence on the weightage by one single risk factor. Further, financial considerations should also not influence the ratings.

The risk rating generated pursuant to the assessment will determine the frequency of the review which the Company should carry out.

The Company shall further review its customer risk profiling methodology to ensure the customer risk categories remain relevant and reflective of the real risk that the Company is exposed to as a result of its customer relationships.

As with the business risk assessment, the client risk assessments, need to be comprehensively documented with the rationale for decisions being clearly explained and recorded.

DD &KYC		
Low	Medium	High Risk Or Deposit > $50,001
Simplified DD (SDD)	Client DD (CDD)	Enhanced DD (EDD)
Reviewed at least annually	Reviewed at least semi-annually	Reviewed at least quarterly
Individual/Corporate	Individual/Corporate	Individual/Corporate

✓ POI+POR	✓ POI+POR ✓ request additional identification document	✓ POI+POR ✓ request additional identification document
✓ Screening and verification	✓ Screening and verification	✓ Screening and verification
		✓Source of Funds Declaration
		✓Source of Funds Supportive Docs

8.2.7.1. Low Risk

In general, the full range of CDD measures should be applied to all applicants. However, where the risk of money laundering or the financing of terrorism is lower and where information on the identity of the applicant is publicly available or where adequate checks and controls exist elsewhere in the national systems, it might be reasonable for the Company to apply simplified or reduced due diligence (the "SDD") measures when identifying and verifying the identity of the applicant.

The Company must ensure that when they become aware of circumstances which affect the assessed risk of the business relationship or occasional transaction, they must undertake a review of the DD documentation and information held with a view to determining whether it is appropriate to continue applying simplified or reduced DD measures.

Where the Company takes a decision to apply SDD measures, documentary evidence which supports the decision must be retained.

However, SDD measures will not be acceptable whenever there is suspicion of money laundering or terrorist financing, or specific higher risk scenarios apply.

Where any aspect of the relationship exposes the Company to an increased level of risk, then SDD measures must not be applied.

8.2.7.2. High Risk

The Company will apply EDD measures as required where it has assessed that the business relationship or occasional transaction is a high-risk relationship, based on the client's individual risk status, that is, the nature of the client, the business relationship, its location, or any other specificity of the business relationship.

9. Non-face To Face Relationship

The business of the Company may also be conducted on a non-face to face basis with clients. Often, it is either impossible or impractical for the Company to have or to obtain original documentary evidence of identity.

However, in such cases, the Company should apply, on a case-by-case basis, as deemed required, the following CDD procedures when dealing with non- face-to face applicants for business:

(a) the certification of documents presented and/or validation via robust system;
(b) the requisition of additional documents to complement those which are required for face to face applicant; and
(c) the initiation of an independent contact with the client.

10.Politically Exposed Person (PEPs)

Domestic PEPs - individuals who are or have been entrusted domestically with prominent public functions in St. Lucia and includes the Head of State and of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

Foreign PEPs – individuals who are or have been entrusted with prominent public functions by a foreign country, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

International organisation PEPs – individuals who are or have been entrusted with a prominent function by an international organisation and includes members of senior management such as directors, deputy directors and members of the board or equivalent functions.

Family members PEPs – are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership. Family members & close associates of PEPs should be determined to be PEPs because of the potential for abuse of relationship for the purpose of Money Laundering& Terrorism Financing (ML&TF).

Close associates of PEPs are individuals who are closely connected to a PEP, either socially or professionally and as such are also deemed PEP.

PEPs are individuals who are or who have been entrusted with prominent public functions (for example Heads of State or of Government, Senior Politicians, Senior Government, Judicial or Military Officials, Senior Executives of State-Owned Corporations and important Political Party Officials, their immediate family members and close associates).

The company should be aware that business relationships with PEPs, family members or close associates of PEPs are deemed to pose a greater than normal money laundering risk by virtue of the possibility for them to have benefited from proceeds of corruption.

The company should thus take additional measures when dealing with such individuals as any scandal associated to them can have major repercussions on their business partners.

Therefore, the company has put in place a policy for the onboarding of these PEPs. The following steps should be followed by the Administrator or company when a PEP is identified or there are any high risk individuals or entities. All PEPs shall be recorded in the Register of PEPs.

Step 1: Collect all due diligence documents on the persons.

Step 2: Perform screening. If screening is clear or does not contain any adverse information move to step 3. On the contrary move to step 4.

Step 3: Provide the Compliance Officer with the screening and due diligence documents so that further internet search can be conducted. If no adverse results are found on the person and all due diligence documents are in order, seek the approval of senior management before accepting the client.

Step 4: Provide the Compliance Officer with the screening and due diligence documents so that further internet search can be conducted. Irrespective if further adverse results are found on the internet, The Compliance Officer will prepare a detailed report with recommendations for senior management to consider approving the onboarding of the PEP.

Step 5: Request further documents or information as approved by the Board.

Step 6: Upon receipt of the information and documents, provide compliance.

PEP related clients will be classified as high risk and the measures applying to a high risk client should be followed.

The Company must ensure to:

(a) obtain the approval of Senior Management prior to establishing relationships with such applicants for business;
(b) where applicants have been accepted and the said applicant or its beneficial owner is subsequently found to be, or subsequently becomes, a PEP, obtain the approval of Senior Management to continue such business relationships;
(c) obtain similar approval from Senior Management in cases of family members or close associates of PEPs;
(d) take enhanced due diligence measures to establish the source of funds and source of wealth of applicants, beneficial owners, family members or close associates of PEPs; and
(e) conduct enhanced ongoing monitoring of the business relationships involving PEPs, family members or close associates of PEPs (including Connected Persons).

The Company must apply appropriate EDD measures on a risk-sensitive basis where an applicant or customer (or any connected person, such as a beneficial owner or controller) is a PEP.

The Company shall apply the same measures for EDD and monitoring in relation to Connected Person as for PEPs.

The Company shall rely on screening systems, i.e., WorldCheck to determine relationships with non- domestic PEPs and Google searches for local PEPs given that there is no repository for local PEPs.

In the event of doubt, the Company may request the services of a third party to perform further checks to determine whether a person is a PEP.

The risks associated with PEPs differ according to the particular countries concerned. The risk of corruption in certain countries is higher than it is in others. The Company do take note of the Transparency International Corruption Perceptions Index at www.transparency.org and take appropriate measures to manage the increased risks of conducting business with PEPs.

When accepting a PEP client, the PEP register will have to be updated.

11.Ongoing Monitoring

The Company conducts the ongoing monitoring review of each business relationship and client file based on their risk rating and any issue raised should be submitted to the Compliance Department.

For example, in relation to the source of funds, the following questions might be asked when determining whether incoming funds may be suspicious:

(a) is the volume and/or size of the transactions consistent with the normal pattern of activity for the client?
(b) is the receipt of the transaction in the context of the client's business or personal activities and their stated commercial objectives?

The risk rating awarded to the client determines the frequency of review by the Compliance Department as follows:

(a) every quarter for High Risk rated clients;
(b) every semester for Medium Risk rated clients; and
(c) every year for Low Risk rated client.

In such cases the Client Services Department should follow up for any outstanding issues as soon as it is made aware of compliance discrepancies (if any), within the appropriate ongoing monitoring time frame.

In the event that clients are not responding to any query or communications or there is a tendency from clients to ignore regulatory/statutory duties or events, the matter must be escalated to the CEO/Managing Director and Compliance as soon as practicable and to prevent any regulatory issue from impacting the Company.

In this event, the CEO/Managing Director will, based on information available and final requests to client, decide on the next steps including resignation in statutory roles and inform the regulator or authorities.

11.1. Transaction Monitoring

The Company shall monitor its business relations with clients on an ongoing basis and observe the conduct of clients' activities and transactions to ensure that they are consistent with its knowledge of the client, its business and risk profile and where appropriate, the source of funds.

The ongoing monitoring of clients' activities and transactions, is a fundamental aspect of effective ongoing DD measures in the identification and mitigation of money laundering, terrorist and proliferation financing risks.

Transaction Monitoring is a process put in place to monitor all transactions and activity of the Company on an ongoing basis, which involves a combination of real-time and post-event monitoring. In the case of real time monitoring, the focus is on transactions/activity where information/instructions are received before a payment instruction is processed. Post-event monitoring consists of reviewing transactions/activity on a periodic basis (e.g. monthly).

The over-riding principle is to ensure that unusual transactions and activity are identified and subject to a heightened level of scrutiny or examination within the shortest delay and properly documented. Where the risks of money laundering, terrorism or proliferation financing are higher, enhanced CDD measures must be conducted which are consistent with the risks identified. Of note, transaction monitoring can trigger an Internal Investigation and warrant a STR report, in case a suspicious transaction is identified.

Transactions will be rated as either of these:

Level 1 - Low Risk

Transactions below a threshold of USD 7,500 or its equivalent in foreign currency will be classified as Low Risk.

Level 2 - Medium Risk

Transactions exceeding a threshold of USD 7,500 or its equivalent, but below that of USD 50,000 or its equivalent will be classified as Medium Risk.

Level 3 - High Risk

Transactions exceeding a threshold of USD 50,000 or its equivalent will be classified as High Risk.

Irrespective of the above classifications and amount, transactions will be classified as high-risk if:

(a) transactions involving clients rated as 'High Risk';
(b) transactions involving PEP clients; or
(c) transactions where transfer instructions and other communications were received from an email address different from that initially provided by the client.

11.1.1. Transaction Monitoring Steps

(d) After client onboarding, the client will deposit funds into the client account of the company.

(e) The Transaction Monitoring Executive will ensure that all DD documents and evidence of screenings and source of funds are on file.
(f) The Transaction Monitoring Executive will go through the bank statement/ any platform set up by the Company on a daily basis regarding inflow and outflow of funds.
(g) If need be, additional documentations will be requested or client will be queried.

FREQUENCY FOR TRANSACTION MONITORING

The Company will formally review all transactions undertaken on a quarterly basis, unless the circumstances require more frequent formal reviews, to ensure that no Financial Crimes have been facilitated or taken place.

12.Suspicious Transactions

Not all unusual or suspicious transactions will actually be cases of money laundering or funds gained from illicit activity. However, there is a duty to report cases that are found to be "suspicious" and let the proper investigations be conducted.

It is extremely important for staff to understand what they are doing and to not do merely do as they are told. Members of staff are requested to use a logical and common-sensical approach and always attempt to decipher the reason for a particular transaction or state of affairs. If something does not make sense or cannot be explained according to the surrounding circumstances of a particular business or transaction, then staff should forthwith notify the CO.

It is the duty of the employee under the law to make a report of any suspicious transaction that he/she comes across and where an employee makes a suspicious transaction report to the CO, he/she will have discharged his/her legal obligation to report to the relevant authority.

The Suspicious Transaction Report (the "STR"), Annex 1, should be remitted directly to the CO or the Alternate CO and not be compromised by any other member of staff within the Company. As soon as the CO receives the report, all details will be logged. The CO shall acknowledge the internal STR.

All KYC details need to be rigorously screened and investigated by the CO to determine the reasonableness of the internal STR. All contributions and memos should be made in writing.

If the investigation can unequivocally be found to be without foundation and not suspicious, then the matter is closed and the findings logged.

If there is any reasonable suspicion, then a full report must be submitted to the authorities not later than five (5) working days from the date the suspicion arose and the relevant details entered the STR log. Accordingly, the client will be classified and treated as high-risk.

The CO will also inform senior management that the clients should be treated as high risk and the risk rating changed accordingly. Senior Management will also ensure that the client is identified as a high-risk and the client is subject to EDD.

12.1. Tipping Off & Malicious Reporting

A. **Tipping Off** is considered a very serious offence by the local regulator. It is the deliberate act of informing the party under suspicion that they are being investigated.
'Tipping off' the client or any other person is a criminal offence and upon conviction, the penalty is a fine and/ or imprisonment.

B. **Malicious reporting**: If anyone submits an STR to the authoritied without reasonable grounds or maliciously, the Company may be sued for breach of client confidentiality. However, if a disclosure is made in good faith but proves to be groundless, then the Company may claim immunity.

12.2. STR Identification, Investigation, Reporting

In order to identify suspicious transactions the CO shall perform the following activities

(a) monitor on a continuous basis any changes in the Client's financial status, business activities, type of transactions etc.
(b) monitor on a continuous basis if any Client is engaged in any of the practices described in the list containing examples of what might constitute suspicious transactions/activities related to Money Laundering and Terrorist Financing.

Furthermore, the CO shall perform the following activities:

(a) receive and investigate information from the Company's employees, on suspicious transactions which creates the belief or suspicion of money laundering. This information is reported on the STR from Annex 1 according. The said reports are archived by the CO
(b) evaluate and check the information received from the employees of the Company, with reference to other available sources of information and the exchanging of information in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained on the report which is submitted to the CO is evaluated on the Internal Evaluation Report according, which is also saved in a relevant file
(c) if, as a result of the evaluation described above, the CO decides to disclose this information to the authorities, then they prepare a written report, which they submit with the authorities.
(d) if as a result of the evaluation described above, the CO decides not to disclose the relevant information to the authorities, then he fully explain the reasons for his decision on the Internal Evaluation Report.

13.Source of Funds /Source of Wealth

In the identification of risk and prevention of money laundering, it is a pre-requisite for the Company to understand the origin or provenance of funds when establishing business relationship with a client. Therefore,

understanding the client's source of funds and the client's source of wealth is an important aspect of client due diligence.

It is important to distinguish between the source of funds and the source of wealth. The "source of funds" is the activity or transaction which generates the funds for a client while the "source of wealth" refers to the activities which have generated the total net worth of the client.

The Company must therefore use a risk-based approach and by taking appropriate measures establish the source of funds for each applicant.

13.1. Source of Funds

Source of Funds (SOF) refers to the origin of funds that an individual or entity uses in a specific transaction or investment. Whether a Source of Funds check is required depends on factors like the customer's risk profile and the guidelines provided by the relevant regulator.

During a SoF check, the Company looks for incoming transactions—or a series of transactions—that can be reasonably explained. To do this, it typically requires bank statements showing these transactions, along with supporting documentation that explains their origin.

For example, if a user states that their source of funds comes from employment, the financial institution will usually request bank statements where the salary payments are visible, as well as an employment contract or payslips to confirm the employer and the amount paid.

Other SOF examples include:

- Proof of Savings
- Salary
- Bonuses and dividends
- Sale agreements (property, assets, investments)
- Inheritance documents or wills
- Winnings from betting/lotteries
- Cryptocurrency transaction records (exchange histories, wallet records)

Whether it's a bank assessing a prospective homeowner's mortgage eligibility or a business meeting routine compliance requirements during account opening or transactions, financial institutions may request different types of Source of Funds (SoF) documents. The level of detail required typically depends on the context and the amount involved, ranging from self-declarations for low-risk or small transactions to documentary evidence for larger or higher-risk amounts. Here are some types of SOF documents that can be requested:

- Financial Documents: Bank statements

- Business Documents: Official documents proving the ownership of the company, company registration documents, stock records, promotional materials, website addresses, any records proving the sale of a business (or dividend payments), and valuation of a business
- Investments: Proof of investment/securities accounts, bank statements, and stock certificates
- Employment: Employment contracts, payslips, and bank statements
- Gift: Documentary proof that funds were received as a gift from a friend, family member, or other entity, bank statements
- Loan: Proof that funds were obtained through a loan from a financial institution, individual, or other sources
- Inheritance: Documents such as a Grant of Probate or a Will
- Real Estate: Documents on real estate purchase/sale, valuation of owned real estate, lease documents on property producing lease income
- Other Source: Documentation on divorce, inheritance, lawsuits, etc.

All of the above documents must explain the source of funds in detail and from various angles. For example, if the customer claims that their funds came from a "gift," a simple note from the person who "gifted" it will not be enough.

This individual will also have to submit:

- Documented proof of funds transfer
- A personal statement explaining the details and circumstances of how the gift was presented
- A signed declaration by the donor explaining what the gift is and its purpose
- Documents proving the source of funds of the individual who made the gift
- Tax return on the gift

In any case, SOF verification is an extremely important aspect of client onboarding, and it is in your power to make it quick and effortless for users.

13.2. Source of Wealth

Source of Wealth (SOW) is a document that provides companies with a broader understanding of the customer's assets and the financial activities that led to their acquisition. An SOW investigation will look at how a customer's wealth was accumulated over time.

Source of Wealth is a more extensive check than Source of Funds and is usually conducted when SoF documents are not sufficient to explain a user's deposit.

For example, if a client deposits €5,000 into an account, the bank may ask where the money comes from. If the user provides an employment contract, payslips, and bank statements showing regular salary payments that align with the deposited amount, this is typically considered a clear and straightforward case.

However, if a client deposits €150,000, the bank will again ask about the origin of the funds, but the user must explain how they accumulated such a large amount. This could include savings built up over several years, proceeds from the sale of property, an inheritance from a deceased relative, or similar sources.

Examples of SOW may include:

- Employment
    - Name and address of the employer
    - Annual salary and bonuses for the last couple of years
    - Last three months /recent payslip (this will depend on the relevant regulation)
    - Confirmation from the employer of the annual salary
    - Latest accounts or tax declaration if self-employed
    - Bank Statements showing transactions
- Business gains from a company sale
    - Copy of the contract of sale
    - Internet research of the Company Registry
    - Name and Address of Company
    - Total sales price
    - Clients' share participation
    - Nature of business
    - The sale date and the receipt of funds
    - Media coverage
- Inheritance of a family fortune
    - Name of deceased
    - Date of death

- Date it was received
- Entire amount
- Solicitor's details
- Tax clearance documents

Demanding SOW is part of Know Your Customer measures, enabling businesses to:

- Expose when clients act for another individual, corrupt official, or family member of a corrupt official
- Provide a bigger picture of the client's background.

14.Termination of the Client

If the client wishes to terminate the Agreement with the Company, the client should formally inform the company in writing. The records of the client will be kept for a period of 7 years.

The Company may terminate the business relationship with the Client at any point in time in accordance with the Client Agreement.

15.AML Training

All employees should be made aware and accept the content of the Company of this Manual.

Employees must be informed of the identity of the CO and the Alternate CO as well as their responsibilities.

The Company needs to ensure that employees who have been provided with the Manual fully understand it and its importance. Employees whose duties relate to the handling of business relationships or transactions, should especially be made aware of these. These employees should receive AML/CFT related trainings at least once a year or as and when changes to the AML/CFT regime are brought.

Directors, managers, Legal & Compliance Executives, Compliance Officer are considered as key employees to whom ongoing training must be given so that they remain competent to give informed and adequate consideration to the evaluation of the effectiveness of the policies, procedures and controls; given that the Board and Senior Management are also responsible for the effectiveness and appropriateness of the Company's policies, procedures and controls to counter money laundering, terrorist and proliferation financing.

Training should be relevant to the role and responsibilities of the employees and may include:

(a) legal obligations as well as aspects of the AML/CFT laws, regulations and guidelines;

(b) the money laundering and terrorist financing vulnerabilities of the products and services offered by the Company;

(c) the DD requirements and the requirements for the internal and external reporting of suspicion;

(d) recognition and handling of suspicious transactions/activities;

(e) the criminal sanctions in place for failing to report information;

(f) new developments including information on current money laundering and terrorist financing techniques, methods, trends and typologies; and

(g) information on the changing behaviour and practices amongst money launderers and those financing terrorisms.

There should be a minimum of at least one training session annually in which all the employees should be participating.

ASSESSMENT OF TRAINING

It is crucial that the Company can assess and ascertain the effectiveness of all training programs put in place. The Company is expected to test or conduct audits of the trainings conducted. Assessment of training programs will be undertaken by using various metrics and which may differ from program to program.

The Board of the Company holds the ultimate responsibility with respect to ensuring that training programs are adequate and meet the prevailing legal and regulatory requirements.

16.Record Keeping

The Company keeps all records in relation to its activities as required by the law. Records comprise of full and true written details of every transaction that the company conducts:

The records are kept:

(a) in physical form or electronic data storage in the computers' hard disc;
(b) or a period of at least 5 to 7 years after the completion of the transaction to which it relates;
(c) at the registered office of the Company or such other place as may be agreed; and
(d) for identification purposes as per the index of each file.

The Company also required to maintain the following records on the suspicious reports being filed:

(a) the internal suspicion reports received by the CO;
(b) records of action taken under the internal and external reporting requirements;
(c) when the CO has considered information or other material concerning the reports, but has not made a disclosure of suspicion to the FIU, a record of the information or material that was considered and the reason for the decision; and
(d) all reports made by the CO to the authority.

The Company is also required to maintain records of all AML/CFT training delivered to employees. Records should include:

(a) the dates AML/CFT training was provided;
(b) the nature of the training, including details of contents and mode of delivery; and
(c) the names of the employees who received training

ANNEXURE I

INDICATORS OF POTENTIALLY SUSPICIOUS ACTIVITY

1. Any doubt over the true identity of an applicant or the principals thereof
2. Any unusual transaction in the context of the normal pattern of activity for a particular relationship
3. Reluctance on the part of clients to respond to enquiries made by the Company
4. Fund transfers to or from accounts in countries that are known to be associated with drug trafficking or other serious crime
5. Clients who produce or demand for collecting large quantities of cash

ANNEXURE II Risk Scoring Matrix

Risk Factor Indicator		Risk Level	Points (1-5)	Comment
Delivery Channel	Non Face to Face	**High**	5	Default for both Existing and New Clients. The respective risk score must be however logged in the Clients assessment record in both scenarios.
	** since we are online broker all clients are coming through the website or social medial channels of the company, therefore by default all clients are in high risk delivery channel category*			
Geographical Risk Rating	Residence in Restricted Countries (e.g., USA, Canada, Afghanistan, Sudan etc.)	**REJECTED**	N/A	For Existing Clients this is probably already known, therefore the risk score may be assigned by default without the Client needing to input the info. . For New Client this info needs to be collected at the onboarding stage to assess. The respective risk score must be however logged in the Clients assessment record in both scenarios.
	Residence in FATF (Jurisdictions under Increased Monitoring)	**HIGH RISK**	5	
	Residence in Sanctioned Countries	**HIGH RISK**	5	
	Residence in High-Risk Jurisdictions subject to a Call for Action	**REJECTED**	N/A	
	Residence in EU /EEA (reverse solicitation)	**LOW RISK**	1	

	Residence in a country which does not fall in any of the above categories	MEDUM RISK	2/3/4	

Actual Deposited amount	USD ($) 250 - 7,500	LOW RISK	1	This info needs to be collected for both Existing and New Clients. The respective risk score must be however logged in the Clients assessment record in both scenarios.
	USD ($) 7,500 - 50,000	MEDUM RISK	2	
	USD ($) 51,000 - 100,000	MEDUM RISK	3	
	USD ($) 101,000 - 200,000	MEDUM RISK	4	
	Greater than USD ($) 201,00	HIGH RISK	5	
	** at initial review and as ongoing factor to review* ** the amount is monitored on a case-by-case basis. Example:* *if a client performs on a single transaction €50,001 and more then EDD will be performed by default as per the RBA and the account will not be able to trade unless full verification process is completed as per the Company's AML Controls.*			

Screening (PEP)	NO	LOW RISK	0	

	Adverse media	case by case	case by case 2/3/4	If already on record for Existing Clients, the risk score may be assigned automatically. The respective risk score must be however logged in the Clients assessment record in both scenarios.
	Yes	**Reject /High****	5	
	** if PEP then Management approval needed.* ** adverse media findings will be examined on a case by case basis* *** 1st degree PEP should be rejected, 2nd and subsequent degree PEPs to be examined case by case*			

Estimated Net Worth (cash, savings, properties, investments, etc.)	USD ($) 0 -50,000	**LOW RISK**	1	If already on record for Existing Clients, the risk score may be assigned automatically. The respective risk score must be however logged in the Clients assessment record in both scenarios.
	USD ($) 51,000 -100,000	**MEDUM RISK**	2	
	USD ($) 101,000 - 300,000	**MEDUM RISK**	3	
	USD ($) 301,000 - 500,000	**MEDUM RISK**	4	
	USD ($) 501,000 -<	**HIGH RISK**	5	

Source of Funds	Salary / Employment Income	**Low**	0/1	This info needs to be collected for both Existing and New

	Pension / Retirement Fund	Medium	2/3	Clients. The respective risk score must be however logged in the Clients assessment record in both scenarios.
	Investment Returns	High	4/5	
	Business Profits	Low	0/1	
	Inheritance	Medium	2/3	
	Other	case by case	case by case	
	** if Other, should be examined on a case by case basis and crosed check according to the market standards*			

LOW RISK	<10
MEDIUM RISK	10 - 24
HIGH RISK	25-30

REJECTED	* if not specifically approved by SM as per AML Controls, where applicable. *If client is from Rejected Countries as per AML Manual. *If after reviewing the risk pertained in the specific relationship is not acceptable by the Company's AML risk apetite