ANTI- MONEY LAUNDERING & COMBATING TERRORISM FINANCING MANUAL

VERSION CONTROL

Owner	Compliance Officer
Version	1.0
Status	Final
Approved by	Board of Directors
Date of last review	02/01/2023

Approved by Board of Directors

Signature

Date

This Anti- Money Laundering & Combating Terrorism Financing Manual ("Manual") is to be strictly adhered to by all employees. There are no exceptions to the Manual without the prior written approval of the Compliance Officer and the Managing Director. Any questions, comments or concerns regarding to the Manual should be directed to the Compliance Officer.

TABLE OF CONTENTS

1. INTRODUCTION 5
2. THE RESPONSIBILITIES OF THE BOARD OF DIRECTORS 6
3. THE RESPONSIBILITIES OF CO 7
4. MONEY LAUNDERING 9
5. TERRORISM FINANCING 11
6. RISK BASED APPROACH 12
7.1 Principles of Risk Based Approach Framework 12
7.2 Identification of Risks 13
7.3 Company Risks 13
7.4 Division into Risk Categories 14
7.4.1 Client Categorisation Criteria- LOW RISK CLIENTS 14
7.4.2 Client Categorisation Criteria- MEDIUM RISK CLIENTS 15
7.4.3 Client Categorisation Criteria- HIGH RISK CLIENTS 15
7.4.4 Client Categorisation Criteria- PROHIBITED CLIENTS 15
7.5 Design and Implementation of Measures and Procedures to Manage and Mitigate the Risks 16
7.6 Suspicious Activities 16
7.6.1 Characteristics to watch for 17
7.6.2 Examples of Potentially Suspicious Scenarios 17
Red Flags related to Due Diligence 17
Red Flags related to Excessive Secrecy 18
Red Flags related to Corporate Structures 18
Red Flags related to Public Officials 18
Red Flags related to Transactions 19
7.6.3 Clients with heightened risk 19
7. THE POLICY AND PROCEDURE FOR REPORTING SUSPICIOUS ACTIVITIES 20
8.1 Reporting Suspicious Activities- Internal Disclosure 20
8.2 Reporting Suspicious Activities- External Disclosure 21
8. CLIENT DUE DILIGENCE AND IDENTIFICATION PROCEDURES 22
9.1 Due Diligence Procedures 22
9.2 List of CDD documents required at the time of penning a trading account 22
9.2.1 In case of Individuals 22
9.2.2 In case of corporate client or firm 23
9.3 Verification of information 23
9.4 Principles of e-KYC Measures 24

9.5 Understanding the Nature and Purpose of Client Relationship 24
9.6 Enhanced Customer Due Diligence ("EDD") 25
9.7 Politically Exposed Persons (PEPs) 26
9. ON- GOING MONITORING PROCESS 28
10.1. General 28
10.2 Procedures 28
10. RECORD KEEPING 30
11. TRAINING 31
12. INDEPENDENTLY TESTING AML PROGRAME 32
13.1 Frequency 32
13.2 Evaluation and Reporting 32
APPENDIX 1- LOG OF HIGH-RISK CLIENTS 33
APPENDIX 2- PEP LOG 34
APPENDIX 3- Acknowledgement Form 35
APPENDIX 4 - 36
APPENDIX 5 – INTERNAL REPORTING FORM 37

1. INTRODUCTION

This Anti- Money Laundering & Combating Terrorism Financing Manual ("Manual") represents the basic standards of Anti-Money Laundering and Combating Terrorism Financing (hereinafter collectively referred to as AML) procedures of UAB BITMARKETS (the "Company"). The Company drafted its Manual in compliance with the applicable law and regulations.

It is aim is to prohibit and actively prevent money laundering and any activity that facilitates money laundering of the funding or terrorist or criminal activities of flow of illegal money.

The Manual among others contains a detailed information on procedures to the followed to ensure compliance related to Know Your Client ("KYC") norms, AML, Client Due Diligence ("CDD") as well as recognition of Suspicious Transactions undertaken by client and reporting requirements to the Financial Intelligence Unit.

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

All amendments and/or changes of the Manual must be approved by the BoD.

2. THE RESPONSIBILITIES OF THE BOARD OF DIRECTORS

The responsibilities of the BoD in relation to the AML prevention include the following:

- to determine, record and approve the general policy principles of the Company in relation to the AML prevention and to communicate them to designated person Anti- Money Laundering Program Compliance Person ("CO") with full responsibility for the Company's AML program;

- 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 CO.

- to approve policies regarding AML/CFT measures within the Company, including those required for risk assessment, mitigation and profiling, CDD, record keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism;

- to ensure that the CO and any other person who have been assigned with the duty of implementing the procedures for the AML prevention, have complete and timely access to all data and information concerning clients' identity, transaction 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;

- to set and ensure effective implementation of appropriate policies and procedures to address the implementation of e-KYC as part of the AML/CFT programme that the Company is required to undertake;

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

- to ensure that the CO has sufficient resources, including competent staff and technological equipment, for the effective discharge of their duties;

- to implement adequate and appropriate systems and processes to detect, prevent and deter AML;

- establish appropriate mechanism to ensure the AML/CFT policies are periodically reviewed and assessed in line with changes and developments in the Company's products, services, technology as well as trends in ML/TF;

- ensure effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML/TF.

3. THE RESPONSIBILITIES OF CO

The responsibilities of the CO in relation to the prevention of AML include the following:

- To detect transactions relating to any crime;
- to design, the internal practice, measures, procedures and controls relevant to the AML prevention, and describe and explicitly allocate the appropriateness and the limits of responsibility of each department that is involved in the abovementioned. It is provided that, the above include measures and procedures for the prevention of the abuse of new technologies and systems providing financial services, for the purpose of AML (e.g. services and transactions via the internet or the telephone) as well as measures so that the risk of AML is appropriately considered and managed in the course of daily activities of the Company and possible changes in the Company's economic profile (e.g. penetration into new markets);
- to ensure a full compliance with the AML Manual, internal policies and procedures, including managing conflicts of interests between the Company and its clients in a manner that ensures the continuity of the Company to perform its business in a sound legal manner.
- to draft effective and appropriate policies and procedures to address the implementation of e-KYC as part of the AML/CFT programme that the Company is required to undertake;
- to review and update the Manual as may be required from time to time, and for such updates to be communicated to the BoD for their approval;
- to monitor and assess the correct and effective implementation of the Manual, the practices, measures, procedures and in general the implementation of the Manual. In this respect the CO shall apply appropriate monitoring mechanisms which will provide him/her with all the necessary information for assessing the level of compliance of the departments and employees of the Company with the procedures and controls which are in force. In the event that the CO identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, gives appropriate guidance for corrective measures and where deems necessary informs the BoD;
- to receive information from the Company's employees which is considered to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities. The information is received in a written report form. This would be Suspicious Transaction Report.
- to evaluate, scrutinise and examine the information received in the Internal Suspicious Report, by reference to other relevant information and discuss the circumstances of the case with the informer and where appropriate, with the informer's superiors. The evaluation of the information of point above shall be done on a report.

- to file Suspicious Transaction Reports (“STR”) and Suspicious Activity Reports (“SAR”) to the Financial Intelligence Unit as appropriate;

- to detect, record, and evaluate, at least on an annual basis, all risks arising from existing and new clients, new financial instruments and services and update and amend the systems and procedures applied by the Company for the effective management of the aforesaid risks;

- to ensure the preparation and maintenance of the list of clients categorized following a risk-based approach, which contains, among others, the names of clients, their account number and the dates of the commencement of the business relationship. Moreover, the CO ensures the updating of the said list with all new or existing clients, in light of any additional information obtained;

- to detect, record, and evaluate, at least on an annual basis, all risks arising from existing and new clients, new financial instruments and services and update and amend the systems and procedures applied by the Company for the effective management of the aforesaid risks;

- to provide advice and guidance to the employees of the Company on subjects related to AML;

- to acquire the knowledge and skills required for the improvement of the appropriate procedures for recognizing, preventing and obstructing any transactions and activities that are suspected to be associated with AML;

- to determine whether the Company's departments and employees that need further training and education for the purpose of preventing AML and organizes appropriate training sessions/seminars. In this respect, CO prepares and applies an annual staff training program. Also, the CO assesses the adequacy of the education and training provided;

- to prepare the monthly, quarterly, biannual and annual reports to the management;

- to follow any new legal and regulatory updates and where necessary ensure its prompt implementation to the Company’s policies and procedures;

4. MONEY LAUNDERING

Money laundering is a generic term used to describe any process that conceals the origin or derivation of the proceeds of crime so that the proceeds appear to be derived from a legitimate source. Money laundering is sometimes wrongly regarded as an activity that is associated only with organized crime and drug trafficking. It is not. It occurs whenever any person deals with another person's direct or indirect benefit from crime. The term 'money laundering' is in fact a misnomer. Often it is not money that is being laundered but other forms of property that directly or indirectly represent benefit from crime. Any form of tangible or intangible property is capable of representing another person's benefit from crime.

The main objective of the money launderer is to transform 'dirty' money into seemingly clean money or other assets in a way to leave as little trace as possible of the transformation. The Company shall adhere to principles established by the Financial Action Task Force ("FATF"), Office of Foreign Assets Control ("OFAC"), United Nations ("UN") and the local regulatory authority which collectively set and enforce standards for anti- money laundering and counter terrorist financing policies and programs.

Failure to comply with these laws, and the regulations that implement them, may result in criminal prosecution. Therefore, employees shall ensure that they adhere to the standards to comply with norms set forth and protect company and its reputation from being misused for any illicit activity.

Traditionally, money laundering has been described as a process that takes place in three stages as follows:

Placement – This is the first stage in 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.

Layering – After successfully injecting the illicit funds into the financial system, laundering them requires creating 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 the illegal source.

Integration – This is the final stage in a complete money laundering operation. It involves reintroducing the illegal funds into the legitimate economy. The funds now appear as clean income. The purpose of the integration of the funds is to allow the criminal to use the funds without raising suspicion that might trigger investigation and pursuit.

In reality, the three stages often overlap and the benefit from many crimes including most financial crimes does not need to be 'placed' into the financial system. The Company is most likely to be exposed at the layering and integration stages of the money laundering process.

Money laundering is a crime that is most often associated with banking and money remittance services. Whilst banks are often an essential part of successful laundering schemes, the financial and related services that the Company offers are also vulnerable to abuse by money launderers. The fight against money laundering is an evolving and never-ending process. Money laundering not only harms the public as a whole, but it shakes the financial services industry. It is clearly in the best interest of the financial industry to take appropriate actions to prevent money laundering.

5. TERRORISM FINANCING

Terrorist financing is the act of providing financial support to acts of terror, terrorists or terrorist organizations to enable them to carry out terrorist acts. Unlike other criminal organizations, the primary aim of terrorist groups is non-financial. Yet, as with all organizations, terrorist groups require funds in order to carry out their primary activities.

This simple fact – the need for funds – is key in fighting terrorism. Follow the money. Follow the financial trail. This is the core objective of all measures that aim to identify, trace, and curb terrorist financing.

There are similarities and differences between money laundering and terrorist financing.

Differences include:

i. Terrorist financing is an activity that supports future illegal acts, whereas money laundering generally occurs after the commission of illegal acts;
ii. Legitimately derived property is often used to support terrorism, whereas the origin of laundered money is illegitimate;

Similarities include:

i. Terrorist groups are often engaged in other forms of criminal activity which may in turn fund their activities;
ii. Both money laundering and terrorist financing require the assistance of the financial sector.

The key to the prevention of both money laundering and terrorist financing is the adoption of adequate CDD measures both at the commencement of every relationship and on an on-going basis thereafter.

6. RISK BASED APPROACH

6.1 Principles of Risk Based Approach Framework

The Company shall apply appropriate measures and procedures, by adopting a risk-based approach, so as to focus its effort in those areas where the risk of AML appears to be comparatively higher.

In this respect the CO shall monitor and evaluate, on an on-going basis, the effectiveness of the measures and procedures of this Section of the Manual. The adopted risk-based approach that is followed by the Company, and described in the Manual, has the following general characteristics:

- recognises that the money laundering or terrorist financing threat varies across clients, countries, services and financial instruments;
- allows the BoD to differentiate between clients of the Company in a way that matches the risk of their particular business;
- allows the BoD 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;
- promotes the prioritisation of effort and actions of the Company in response to the likelihood of AML occurring through the use of the Services the Company is licensed to offer.

The risk-based approach adopted by the Company, and described in the Manual, involves specific measures and procedures in assessing the most cost effective and appropriate way to identify and manage the AML risks faced by the Company.

Such measures include:

- identifying and assessing the AML risks emanating from particular clients or types of clients, financial instruments, services, and geographical areas of operation of its clients;
- managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls;
- continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

The application of appropriate measures and the nature and extent of the procedures on a risk-based approach depends on different indicators.

Such indicators include the following:

- the scale and complexity of the services offered;
- geographical spread of the services and clients;
- the nature and economic profile of clients as well as of financial instruments and services offered;
- the distribution channels and practices of providing services;
- the volume and size of transactions;
- the degree of risk associated with each area of services;
- the country of origin and destination of clients' funds;
- deviations from the anticipated level of transactions;
- the nature of business transactions.

The CO shall be responsible for the development of the policies, procedures and controls on a risk-based approach. Further, the CO shall also be responsible for the implementation of the policies, procedures and controls on a risk-based approach.

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. The Company shall assess and evaluate the risks it faces, for the use of the services it is licensed to offer for the purpose of the AML. The particular circumstances of the Company determine suitable procedures and measures that need to be applied to counter and manage risk.

The Company shall be, at all times, in a position to demonstratethat the extent of measures and control procedures it applies are proportionate to the risk it faces for the use of the services, for the purpose of AML.

6.3 Company Risks

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

i. *Risks based on the client's nature:*

- complexity of ownership structure of legal persons;
- companies incorporated in offshore centres;
- politically exposed persons ("PEPs");
- clients engaged in transactions which involves significant amounts of cash;
- clients from high risk countries or countries known for high level of corruption or organised crime or drug trafficking;
- clients included in the leaked documents of Mossack Fonseca (Panama Papers);
- clients convicted for a predicate offence (and already served their sentence);
- unwillingness of client to provide information on the beneficial owners of a legal person.

ii. *Risks based on the client's behaviour:*

- client 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 clients to provide information on the beneficial owners of a legal person.

iii. *Risks based on the client's initial communication with the Company:*

- non-face-to-face client requests;
- clients introduced by third person.

iv. *Risks based on the Company's services and financial instruments:*

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

6.4 Division into Risk Categories

Having performed the risk assessment based on the criteria described above, the CO then determines which clients fall into categories of low, medium, high risk or prohibited clients/Unacceptable. All clients are risk rated at the time of "onboarding" and periodically thereafter, depending on the initially attributed risk rating. High risk clients will be subject to additional monitoring and will be red flagged.

The Company uses the following classifications:

- Low Risk;
- Medium Risk;
- High Risk;
- Prohibited Clients/Unacceptable Clients;

6.4.1 Client Categorisation Criteria- LOW RISK CLIENTS

The Company may apply simplified due diligence to the following types of Clients provided that this a low risk or no suspicion for AML.

- When the Company listed companies, whose securities are admitted to trading on a regulated market in a country a country which is subject to disclosure requirements;
- Domestic public authority;
- Regulated financial institution.

It is provided that, further to the cases mentioned above, the Company has to gather sufficient information to establish if the client qualifies as a low-risk client. In this respect, CO shall be responsible to gather the said information. The said information shall be duly documented and filed, as applicable, according to the recording keeping procedures.

6.4.2 Client Categorisation Criteria- MEDIUM RISK CLIENTS

The following types of Clients can be classified as medium risk Clients with respect to the AML risk which the Company faces:

- any Client who does not fall under the 'low risk Clients' or 'high risk Clients' categories.

6.4.3 Client Categorisation Criteria- HIGH RISK CLIENTS

The following types of clients can be classified as high risk clients with respect to the AML risk which the Company faces:

- **all non-face-to- face clients;**
- trust accounts;
- 'Client accounts' in the name of a third person;
- PEPs' accounts;
- Clients from countries which inadequately apply FATF's recommendations;
- Clients included in the leaked documents of Mossack Fonseca (Panama Papers);
- Clients convicted for a predicate offence (and already served their sentence);
- cross-frontier correspondent banking relationships with credit institutions-clients from third countries;
- any other clients that their nature entail a higher risk of AML;
- any other Client determined by the Company itself to be classified as such.

6.4.4 Client Categorisation Criteria- PROHIBITED CLIENTS

Prohibited clients include:

- Any client whose name appears on the List of Specially Designated Nationals and Blocked Persons maintained by the U.S. Office of Foreign Assets Control ("OFAC"), which may be found at http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx;
- Common Foreign & Security Policy of the European Union, which may be found at http://eeas.europa.eu/cfsp/sanctions/consol-list_en.htm;
- Any client whose name appears on World-Check, which may be found at http://www.world-check.com, or equivalent client screening applications;
- Foreign Shell Banks;

- Clients who are involved in electronic gambling/gaming activities through the internet;
- High-risk clients that have not satisfied enhanced CDD requirements;
- Such other lists of prohibited persons and entities as may be mandated by applicable laws or regulations, or maintained internally;
- Nationals of Afghanistan, Cuba, Noth Korea, Crimea, Israel, Sudan, Bosnia a Herzegovina, Ethiopia, Iran, Iraq, Lao's People Democratic Republic, Syria, Uganda, Vanuatu and Yemen.

6.5 Design and Implementation of Measures and Procedures to Manage and Mitigate the Risks

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

These measures and procedures include:

- adaption of the CDD Procedures in respect of clients in line with their assessed AML risk;
- requiring the quality and extent of required identification data for each type of client to be of a certain standard (e.g. documents from independent and reliable sources, third person information, documentary evidence);
- obtaining additional data and information from the clients, where this is appropriate for the proper and complete understanding of their activities and source of wealth and for the effective management of any increased risk emanating from the particular business relationship or the occasional transaction;
- ongoing monitoring of high-risk clients' transactions and activities, as and when applicable.

In this respect, it is the duty of the CO to develop and constantly monitor and adjust the Company's policies and procedures.

6.6 Suspicious Activities

As the types of transactions which may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. Suspicion is personal and subjective and falls far short of proof based on specific evidence. However, it is more than the absence of certainty that someone is innocent. Where there is a business relationship, an unusual or suspicious transaction will often be one which is inconsistent with a client's known legitimate business profile or personal activities or with the normal business for that type of relationship. Therefore, the first key to recognition is 'knowing enough' about the client and his/her business to recognise whether a transaction or series of transactions is unusual.

6.6.1 Characteristics to watch for

There are a number of characteristics which are a common feature of money laundering activity.

Some of these are:

- Reluctance to provide basic information to verify identity;
- Engaging in transactions which do not make commercial sense;
- Transactions out of character with the business expected or with the history of the relationship;
- Reluctance to clearly explain source of funds;
- Transfers to/from parties unrelated to the account holder without proper explanation;
- Multiple similar transactions that could have been more effectively combined; transactions spanning many jurisdictions with no obvious reason.

The existence of one or more of the above characteristics does not automatically mean that a client is a money launderer. However, they are an indication that something may be wrong and should give rise to further scrutiny. The client may have a perfectly good reason for the unusual characteristics which would allay any suspicion.

The CO shall coordinate a periodic risk-based review of the Company's existing clients in order to verify that no client is a Prohibited Client, as defined below, and to ensure the adequacy of the ongoing CDD performed on existing clients. The review is performed at least annually or as often as deemed appropriate by the CO.

If such a suspicious activity is detected the Company requires of any employee, who detects suspicious activity or has reason to believe that suspicious activity is taking place, to immediately inform the CO. Under no circumstances may an employee discuss the suspicious activity, or the fact that it has been referred to the CO, with the client concerned. The CO shall determine whether to report to appropriate law enforcement officials any suspicious activity of which he/she becomes aware.

6.6.2 Examples of Potentially Suspicious Scenarios

The following are examples of unusual or suspicious transactions, sometimes called "red flags". Staff should be aware that unusual behaviour could occur at any time during a relationship with a client. The list is not exhaustive but is provided to assist staff in understanding transactions which could be unusual when compared against a client's expected pattern of activity.

Red Flags related to Due Diligence

- Clients who exhibit unusual concern in regard to compliance, with reporting requirements and the Company's anti-money laundering policies, particularly

with respect to his/her identity, type of business and assets, reluctance or refusal to reveal any information concerning business activities;
- Information provided by the client that identifies a legitimate source for funds is false, misleading, or substantially incorrect;
- Clients who (or a person publicly associated with the client) have a questionable background or are the subject of news reports indicating possible criminal, civil, or regulatory violations;
- The client's activity demonstrates outflows of funds or other assets well beyond the known income or resources of the client;
- Unsatisfactory or incomplete identification evidence;
- Reluctance or a refusal by a client to provide complete identification evidence;
- Clients asking staff to "bend" the rules;
- Unwillingness to disclose the source of funds;
- Unwillingness to disclose the identity of ultimate beneficial owners;
- Lack of adequate identification or source of funds being provided;
- Any action or request by a client which is inconsistent with your experience or knowledge of their business, affairs, income or previous history;
- The receipt or transmission of funds in circumstances which appear to have no commercial logic or perhaps involve jurisdictions which are renowned for money laundering;
- Client who is a known or suspected triad member, drug trafficker or terrorist or where the client has been introduced by any such persons;
- Situations where the identity of the client is difficult to be determined;

Red Flags related to Excessive Secrecy

- Unnecessary granting of powers of attorney, in particular wide-ranging powers of attorney;
- Using different accounts to transfer the funds directly;
- A client tries to persuade an employee not to file required reports or maintain required records;
- A client is reluctant to provide information needed to file an internal report, in compliance with the requirements of legislation.

Red Flags related to Corporate Structures

- Subsidiaries which have no apparent purpose;
- Companies which continuously make substantial losses;
- Complex group structures without a cause;
- Uneconomic group structures for tax purposes;
- Frequent changes in shareholders and directors.

Red Flags related to Public Officials

- Clients who are public officials conducting business in the name of a family member who begins making large transfers not consistent with the known legitimate sources of income of the family;
- Clients who are related to public officials and make large transfers not consistent with his/her own legitimate sources of income.

Red Flags related to Transactions

- Transactions that appear inconsistent with a Client's known profile or unusual deviations from normal transaction or relationship;
- Transactions that require the use of complex and opaque entities and arrangements;
- Transactions with entity established in jurisdictions with weak or absent AML/CFT laws and/or secrecy laws;
- The entry of matching buys and sells in particular securities, creating illusion of trading. Such trading does not result in bona fide market position, and might provide "cover" for a money launderer'
- Buying and selling of a security with no discernible purpose or in circumstances, which appear unusual
- Larger or unusual settlements of securities transactions in cash form.

6.6.3 Clients with heightened risk

Certain types of clients may inherently carry a heightened integrity risk, for example, operators of coffeeshops or commercial real estate activities. This is because the origins of the large amounts of incoming cash are harder to determine thus, they carry a higher risk of fraud and money laundering. This means that the Company needs to take additional measures for these kinds of clients in order to mitigate the risk.

7. THE POLICY AND PROCEDURE FOR REPORTING SUSPICIOUS ACTIVITIES

7.1 Reporting Suspicious Activities- Internal Disclosure

Any information or other matter which gives rise to a knowledge or suspicion that a client is engaged in or attempting to engage in money laundering, terrorist financing or any other crime has to be reported to CO as soon as possible by completing the Internal Reporting Form ("Form") (Appendix 6).

Documenting one's suspicions ensures that the staff members and the Company are protected from criminal liability for failure to report. It is important that staff members do not delay documenting their concerns immediately. This can assist CO, and FIU, to act quickly and within the requirements of the applicable law.

After completing the Form, the staff member should sign and date it, obtain the signature of CO and receive a copy of the Form for their files. CO will acknowledge receipt of such reports and remind the staff member concerned not to do or say anything which might alert the client that he/she/it may be under investigation.

CO will then access the Form and he/she will decide whether a report should be made to FIU. In the case where the CO decided that there are no reasonable grounds for suspicion, the CO will then file the decision, supported by the relevant documents. The report of CO will be thereafter kept as per the Record Keeping Policy of the Company.

Amongst other things CO will consider:

- If any of the 'red flags' have been identified;
- Deviating behaviour on the part of the client, and activities that are illogical based on knowledge of the client or sector;
- The client makes use of legal persons or companies in which the control structure is not transparent or which, because of their nature or method of incorporation, are suitable for masking the identity of the underlying beneficial owner (e.g. bearer shares, trusts, foreign legal persons), without being able to give the Company an acceptable explanation for this;
- The frequent alteration of legal structures and/or changing of directors of legal persons or companies. There is a complex legal structure that does not appear to serve a genuine object;
- Transactions have no clear economic purpose;
- Transactions appear to be illegal;
- Transactions involve proceeds from an unlawful activity;
- Transactions indicate that the client is involved in ML/TF.
- In addition to the indicators, the 'gut feeling' of employees and CO is also important.

It is very important that Internal and External Reporting Forms are kept in files that are entirely separate from those of the client. It is the responsibility of the CO to maintain and kept securely these files.

Failure to report suspicious activities or having a knowledge that the funds deposited in the Trading Account of Client are proceeds of felony or a misdemeanour and/or anyone who wilfully commits any of the following acts, shall be considered a perpetrator of the crime of money laundering:

- Transferring or moving proceeds or conducting any transaction with the aim of concealing or disguising their Illegal source.
- Concealing or disguising the true nature, source or location of the proceeds as well as the method involving their disposition, movement, ownership of or rights with respect to said proceeds.
- Acquiring, possessing or using proceeds upon receipt.
- Assisting the perpetrator of the predicate offense to escape punishment.

Therefore, a failure to report suspicious activities is a serious failure that may cause imposition of penalties and or crime sentence based on the severity of the crime.

All employees who report the suspicious activities are protected by law by filing an Internal Suspicious Report Form. As such the Company warrants the following:

> ***"No action, suit, prosecution or other proceedings shall lie be be brought, instituted or maintained in any Count or any tribunal or proceedings against the staff who report such violation or non-compliance provided that such act was made in good faith."***

7.2 Reporting Suspicious Activities- External Disclosure

The CO has the sole discretion and independence to report suspicious transactions. These reports must be submitted with utmost care and threated with the highest level of confidentiality.

The CO must ensure that the suspicious transaction report is submitted within next working day, from the date the CO establishes the suspicion.

8. CLIENT DUE DILIGENCE AND IDENTIFICATION PROCEDURES

8.1 Due Diligence Procedures

The following CDD indicates the criteria for acceptance of clients must be followed at all times:

- Identify the prospective client and verify that prospective client's identity using reliable, independent source documents, data or information;
- Verify that any person purporting to act on behalf of the prospective client is so authorised, and identify and verify the identity if that person;
- Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the reporting institution is satisfied that it knows who the beneficial owner is, and
- Understand and, where relevant, obtain information on the purpose and intended nature of the business relationship;
- If a prospective client does not provide a complete information, the trading account cannot be opened;
- No trading account can be opened where the Company is unable to apply appropriate CDD measures and procedures.

8.2 List of CDD documents required at the time of penning a trading account

8.2.1 In case of Individuals

- Full Name;
- A copy of valid National Registration Identity Card; or
- A copy of passport;
- A copy of any other photo identity card;
- Proof of Current Address no older than three (3) months- any one of:
    - ✓ An original utility bill;
    - ✓ A bank statement or credit card statement showing name and address;
    - ✓ Bank reference;
- Residential and mailing address;
- Date of birth;
- Nationality;
- Occupation type;
- Name of employer or nature of self-employed/nature of business
- The purpose of transaction;
- Source of wealth;
- Contact number;
- Any other CDD documents that may be required by CO.

8.2.2 In case of corporate client or firm

All the below mentioned should be provided as certified/notarised copies of originals

- Understand the nature of the prospective client business, its ownership and control structure;
- Name of the company;
- Memorandum of Articles of Association;
- Certificate of incorporation;
- A passport copies of authorised signatory (if other than UBO or directors);
- Company bank statement;
- Latest audited financial statements;
- Electricity/Water or a landline bill of authorised signatory no older than three (3) months;
- A copy of utility bill showing the registered office address (no older than three months) or company bank statement clearly showing the registered address the registered address of the corporate or firm;
- Copy of passport/ID card of all directors/partners as the case may be;
- Copy of passport/ID card of all beneficial owners (up to the ultimate beneficial owner) as the case may be;
- Copy of residential addresses of all directors/partners as the case may be no older than three (3) months;
- Copy of residential addresses of beneficial owners (up to the ultimate beneficial owner) as the case may be no older than three (3) months;
- Source of funds- company bank statements;
- A board resolution authorising the authorised individuals to act on behalf of corporate;
- Any other CDD documents as may be requested at discretion of CO.
- All UBOs must be identified regardless of the percentage they hold (e.g. even if it is 1%)

8.3 Verification of information

Based on the risk, and to the extent reasonable and practicable, the Company will ensure that it has a reasonable belief that it knows the true identity of its clients by using risk-based procedures to verify and document the accuracy of the information it gets about its potential clients. CO will analyze the information that is obtained in order to determine whether the information is sufficient to form a reasonable belief that the Company knows the true identity of a potential client.

The information will be verified within a reasonable time, before the trading account is opened. If the Company finds suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, it will, after internal consultation with the CO, file a Suspicious Transaction Report in accordance with applicable laws and regulations.

In circumstances when the Company cannot form a reasonable belief that it knows the true identity of a potential client, it will (1) not open an account; (2) determine whether it is necessary in accordance with applicable laws and regulations to file a Suspicious Transaction Report.

At the time of opening a trading account for a legal entity customer, the Company identify any individual that is a beneficial owner of the legal entity by identifying any individuals who directly or indirectly own 5% or more of the equity interests of the legal entity, and any individual with significant responsibility to control, manage, or direct a legal entity customer. The following information will be collected for each beneficial owner:

- the name;
- date of birth (for an individual);
- an address,
- an identification ID,

8.4 Principles of e-KYC Measures

The Company will take int account the following minimum measures in the e-KYC solution to identify and verify a client's identity.

- Establishing that the information about the client's identity is provided from a trusted database; or

- If the information about the client's identity is not provided from a trusted database, the e-KYC solution has to perform documentation verification and biometric authentication; or

- Collecting client's information for the purpose of validating the identity, which includes:
  i. Performing a live scan of the client's identity document; and
  ii. Taking live photos (or live video) of the customer.

- When subscribing to any e-KYC system provided by a third-party service provider, the LFIs remain accountable in ensuring effective CDD is undertaken which adheres to the above principles.

8.5 Understanding the Nature and Purpose of Client Relationship

The Company needs to understand the nature and purpose of client relationships for the purpose of developing a customer risk profile through the following methods.

Depending on the facts and circumstances, a customer risk profile may include such information as:

- The type of customer;
- The account or service being offered;
- The customer's income;
- The customer's net worth;
- The customer's domicile;
- The customer's principal occupation or business; and
- In the case of existing customers, the customer's history of activity.

8.6 Enhanced Customer Due Diligence ("EDD")

EDD will be undertaken by the CO in the following situations:

- possible match on a Sanctions list. The profile for the potential match indicates negative information and the anti-money laundering ("AML")/know your customer ("KYC") screening software hit cannot be definitively ruled out as a true match;

- PEP match. The potential match is classified by the AML/KYC screening software as a PEP. An immediate family member of such person or a known close associate of such person also qualifies as a PEP.

- questionable jurisdiction connection. The person is a citizen of a country of questionable repute or without adequate anti-money laundering strategies or resides there. The countries which qualify as "questionable" are determined by the CO from time to time, having regard to a number of resources, including the FATF recommendations;

- questionable business activity. The person is involved in industries that are of questionable reputation, such as casinos or pornography, or is involved in a business that is highly cash intensive. Which business activities are questionable are determined by the compliance department from time to time, having regard to a number of resources, including the FATF's recommendations;

- where jurisdictions have been identified by the FATF as jurisdictions that have not set up adequate systems to prevent money laundering and terrorist financing, this is seen as one of the factors increasing the risk of money laundering and terrorist financing in a business relationship.

EDD shall be undertaken by obtaining additional information on the prospective client and/or beneficial owner. The following list below provides some examples:

- volume of assets, occupation, and other information from reliable public database;
- inquiring on the source of wealth or source of funds. In case of PEPs, both sources must be obtained;
- obtaining approval from the senior management of the Company before establishing (or continuing for existing client) such business relationship with the prospective client. In the case PEPs, approval from the highest senior management is required;

- obtaining additional information on the intended level and nature of the business relationship;
- updating more regularly the identification data of client and beneficial owner;
- inquiring on the reasons for intended or performed transactions;
- requiring the first payment to be carried out through an account in the client's name with a banking institution subject to similar CDD standards.

All High-Risk clients will be recorded in the High Risk Clients Log (Appendix 1).

8.7 Politically Exposed Persons (PEPs)

A politically exposed person (PEP) is defined by the Financial Action Task Force (FATF) as an individual who is or has been entrusted with a prominent public function, as well as the immediate family members or close associates of these individuals. Due to their position and influence, it is recognised that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering offences and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing.

In light of the above when the Company enters into a business relationship with or provides services to PEPs additional identification measures must be taken as the business relationships entails a higher risk. The Company applies risk-based procedures and measures in order to be able to identify PEPs, and consequently determine the source of wealth and of funds that are used with the business relationship and keep the business relationship under constant review.

A review is carried out both on acceptance and periodically to determine whether the client and the UBO qualify as PEPs. This applies equally to natural persons who may exert considerable influence on, hold considerable interests in and/or may strongly influence further reaching decisions of the unincorporated partnership, or who are able to control the partnership's policy to an essential degree. The depth of the due diligence varies depending on the risk profile of the client or UBO. In order to determine whether a particular client or UBO is a PEP, the Company amongst others steps performs number of screening lists internally prepared by the Financial Institutions, lists issued by the local as well as international regulatory authorities such as notices from OFAC, UN as well as it uses World Check application.

All searches are then filed in the client's compliance file. The final decision to enter into a business relationship with PEP or to conduct a transaction for PEP must always be approved by the CO and the BoD. This also applies to a decision to continue a relationship with a customer who becomes PEP. Such approval is granted by the CO and the BoD. All PEPs will also be subject to ongoing monitoring.

All PEPs will be recorded in the PEPs Log (Appendix 2).

Any suspicious and/or unusual transaction to be reported to the FIU. The Compliance Department is responsible to file Suspicious Transaction Report (“STR”) with the Financial Intelligence Unit.

9. ON- GOING MONITORING PROCESS

9.1 General

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

The constant monitoring of the clients' accounts and transactions is an imperative element in the effective controlling of the risk of AML. In this respect, the CO shall be responsible for maintaining as well as developing the on-going monitoring process of the Company.

9.2 Procedures

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

i. the identification of:
   - all high-risk clients, as applicable;
   - the Company shall be able to produce detailed lists of high-risk clients, so as to facilitate enhanced monitoring of accounts and transactions, as deemed necessary;
   - transactions which, as of their nature, may be associated with money laundering or terrorist financing;
   - unusual or suspicious transactions that are inconsistent with the economic profile of the client for the purposes of further investigation;
   - in case of any unusual or suspicious transactions, the person who identified the unusual or suspicious transactions shall be responsible to communicate with the CO;

ii. further to point (i) above, the investigation of unusual or suspicious transactions by the CO. The results of the investigations are recorded in a separate memo and kept in the file of the Clients concerned;

iii. the ascertainment of the source and origin of the funds credited to accounts;

iv. the on-going monitoring of the business relationship in order to determine whether there are reasonable grounds to suspect that client accounts contain proceeds derived from serious AML and/or tax offences;

v. the use of appropriate and proportionate IT systems including:
   - adequate automated electronic management information systems which will be capable of supplying the BoD and the CO, on a timely

basis, all the valid and necessary information for the identification, analysis and effective monitoring of client accounts and transactions based on the assessed risk for AML purposes, in view of the nature, scale and complexity of the Company's business and the nature and range of the investment services undertaken in the course of that business;

- automated electronic management information systems to extract data and information that is missing regarding the Client identification and the construction of a Client's economic profile;

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

vi. the monitoring of accounts and transactions in relation to specific types of transactions and the economic profile, as well as by comparing periodically the actual movement of the account with the expected turnover as declared at the establishment of the business relationship. Furthermore, the monitoring covers clients who do not have a contact with the Company as well as dormant accounts exhibiting unexpected movements;

vii. the frequency of the on-going due diligence or enhanced on-going due diligence, as the case may be, shall commensurate with the level of ML/TF risk posed by the client based on the risk profiles and nature of transactions.

10. RECORD KEEPING

All records relating to internal decision-making, policy formulation, all documents obtained for the purpose of identification and all transaction data as well as other information related to money laundering matters, suspicious activity reports, records of AML/CTF training sessions shall be safeguarded in such a way that only authorized employees have access to this information and documentation as well as in accordance with the applicable anti-money laundering laws/regulations.

All records will be stored either digitally or on paper, depending on the form in which information and documentation is available.

The records shall be stored in such a way that:

i at the request of a supervisory institution, the data/information required is easily accessible and will provide sufficient evidence;
ii any changes and modifications to the content can be easily identified;
iii the information cannot be manipulated or altered.

All records must be kept for period of not less than six years from the date of expiration/termination of the contractual relationship with the Client.

For further information please refer to the Record Keeping Policy.

11. TRAINING

In view of the complexity of the business activities and the increased level of regulatory requirements that the Company is required to comply with, it is imperative that all the employees maintain a good level knowledge that enables them to effectively discharge their responsibilities. In particular, adequate knowledge and experience on the part of employees concerning the management of the risks of AML and ensuring a full compliance with the legal framework is something that the Company takes very seriously.

Thus, the employees regularly attend educational courses which indispensable for their future development. The training programmes are focused not only on the legal and compliance framework within which the Company is required to operate but also on AML techniques, methods and trends, on the international context and standards, and on new developments.

Further, in order to assist employees in understanding of all policies and procedures, the Company provides anti money laundering and terrorism financing training sessions for employees. Attendance is required for all employees. The CO will keep records of all training sessions, including dates, times, locations and names of attendees.

All new staff will also receive an introduction to compliance and AML training by the CO as soon as reasonably practical after joining the Company. This training will be arranged by the CO.

All relevant staff also received a regular refresher training to ensure that their knowledge is kept current with recent developments. The CO will organise and co-ordinate the necessary compliance training. The CO will also assess the need for further training.

Furthermore, all employees are expected to be fully aware of the Company's policies and procedures. Each employee is required to read and comply with the Manual, address any questions and concerns to the CO or and sign the acknowledgement form Appendix 3 confirming that he/she has read, understood and will comply with the Company's policies and procedures.

The Company maintains an ongoing Training Register, as set out in Appendix 4. Training records are kept for the minimum period of six (6) years.

For further details please refer to the Induction Training Policy and Internal Training Policy.

12. INDEPENDENTLY TESTING AML PROGRAME

As a general matter, independent testing of the Company' AML compliance program should include, at a minimum:

- evaluating the overall integrity and effectiveness of our firm's AML compliance program;
- evaluating our firm's procedures for FIU reporting and recordkeeping requirements;
- evaluating the implementation and maintenance of the Company's CDD;
- evaluating our firm's CDD requirements;
- evaluating our firm's transactions, with an emphasis on high-risk areas;
- evaluating the adequacy of the Company's staff training program;
- evaluating the Company' systems, whether automated or manual, for identifying suspicious activity; (8) evaluating our firm's system for reporting suspicious activity;
- evaluating our firm's policy for reviewing accounts that generate multiple SAR-SF filings;
- evaluating the Company' response to previously identified deficiencies.

12.1 Frequency

The testing of our AML program will be performed at least annually.

12.2 Evaluation and Reporting

After the Company has completed the independent testing, staff will report its findings to senior management. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

APPENDIX 1- LOG OF HIGH-RISK CLIENTS

First Name	Middle Name	Surname	Client Number	Date Added	Reason for "high risk client status"

APPENDIX 2- PEP LOG

First Name	Middle Name	Surname	Client Number	Date Added	Reason for "PEP status"

APPENDIX 3- Acknowledgement Form

I, the undersigned, acknowledge that I have received, have read and have understood the Anti – Money Laundering Manual and Combating Terrorism Financing (the "Manual"). I will adhere to the policies and procedures set forth in the Manual. I have had an opportunity to clarify any questions, which I may have concerning the provisions of the Manual.

I further understand that the principles herein may be changed from time to time at the discretion of the CO with prior approval of the Board of Directors.

Employee name	Employee signature	Date

APPENDIX 4 - Training Attendance Sheet

I, the undersigned, hereby confirm that I have attended the AML Staff Training which included inter alia information about prevention and suppression of AML, related legislation, offences, supervisory authorities, examples of AML, Company's updated AML Manual, due diligence procedures with respect to high-risk clients provided by Company's Anti-Money Laundering Compliance Officer.

No.	Date	Department	Full Name	Signature
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

APPENDIX 5 – INTERNAL REPORTING FORM

Internal Reporting Form		
Your name and contact details:	Name	
	Department and position	
	Address	
	Tel No.	
	Email	
	Date	
The names of those involved (if known):		
Details of concerns:		
(Please provide full details of the suspicious activity: names, dates and places and the reasons why you consider this to be a suspicious activity together with any supporting evidence. Please continue on separate sheet if necessary.		

Full Name of the Employee	
Signature	
Date and Place	

Full Name of the Compliance Officer	
Signature	
Date and Place	