Moneta Markets Ltd. ("We", "the Company" or "Moneta Markets")

Prevention of Money Laundering & Terrorist Financing Manual

Version: March 2023

Content

1. General Definitions

For the purposes of this Manual, unless the context shall prescribe otherwise:

"Advisory Authority" means the Financial Services Regulatory Authority

"Act" means the Money Laundering Prevention Act, 2010;

"Beneficial Owner" as shall include:

(a) in the case of a legal entity, any individual who —

i. exercises control over the management of the legal entity;

ii. in respect of a legal entity other than a legal entity whose securities are listed on a recognised exchange, owns or controls, directly or indirectly, more than 25 percent of the shares or voting rights in the body corporate or legal entity;

(b) in the case of a partnership, any individual who —

i. ultimately is entitled to or controls, directly or indirectly, more than 25 percent of the capital or profits of the partnership or more than 25 percent of the voting rights in the partnership; or

ii. otherwise exercises control over the management of the partnership;

(c) in the case of a trust,

i. any individual who is entitled to a specified interest in at least 25 percent of the capital of the trust property;

ii. the class of persons in whose main interest the trust is set up or operates except where the trust is set up or operates entirely for the benefit of the individuals referred to in subparagraph (i);

iii. any individual who has control over the trust.

(d) in the case of a legal entity, partnership or trust other than one referred to in paragraph (a), (b) or (c) —

i. where the individuals who benefit from the legal entity, partnership or trust have been determined, any individual who benefits from at least 25 percent of the property of the legal entity, partnership or trust;

ii. where the individuals who benefit from the legal entity partnership or trust are yet to be determined, the class of persons for whom the legal entity, partnership or trust is set up or operates;

iii. any individual who exercises control over at least 25 percent of the property of the legal entity, partnership or trust.

"Business Relationship" means any arrangement made between a person and a reporting entity where:

(a) the purpose or effect of the arrangement is to facilitate an occasional, frequent, habitual or regular course of dealing between the person and the reporting entity; and

(b) the total amount of any payment to be made by any person to any other person in the course of that arrangement is not known or capable of being ascertained at the, time the arrangement is made;

"Company" means Moneta Markets Ltd., an international business company registered in Saint Lucia under registration number: 2023-00068.

"Correspondent banking" means the provision of banking services by one bank to another bank"

"**Customer",** in relation to a transaction or an account, includes –

(a) the person in whose name a transaction or account is arranged, opened or undertaken;

(b) a signatory to a transaction or account;

(c) any person to whom a transaction has been assigned or transferred;

(d) any person who is authorised to conduct a transaction; or

(e) such other person as may be prescribed;

"Criminal Activity" constitutes any act or omission against any applicable law.

"Data" means representations in any form of information or concepts;

"Financing of Terrorism" is an offence established when a person (by means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they will be used in full or in part, in order to carry out a terrorist act or activity

"Money Laundering" is a process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. Money laundering enables criminals to maintain control over their illicit proceeds and ultimately to provide legitimate cover for the illegal source of the illicit proceeds. This means that proceeds from criminal activities is converted into assets that gives it an appearance of legitimate money.

Money laundering is an international scourge and the failure by the authorities to prevent the laundering of the proceeds of crime will enable criminals to benefit from their illegal activities, thereby making crime a viable proposition.

"Occasional Transaction" means any transaction involving cash that is conducted by any person other than through an account in respect of which the person is the customer.

"Politically Exposed Person (PEP)" means persons holding prominent public positions in a foreign country such as heads of state or government, senior politicians on the national level, senior government, judicial, military or party officials on the national level, or senior executives of State-owned enterprises of national importance, or individuals or undertakings identified as having close family ties or personal or business connections to the aforementioned persons.

"Property" means currency and assets of any kind, whether corporeal or incorporeal, movable or immovable and legal documents or instruments in any form including electronic or digital, evidencing title to or interest in such assets, including but not limited to bank credits, travelers' cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit, whether situated in Saint Lucia or elsewhere and includes any legal or equitable interest in any such property

"Regulated Person"

(a) a regulated reporting entity other than a bureau De change; or

(b) a foreign regulated person.

"Regulations" means the applicable laws in Saint Lucia.

"Shell Bank" is a bank, or an institution engaged in equivalent activities, that

(a) is incorporated in a country in which it has no physical presence involving meaningful decision-making and management; and

(b) is not subject to supervision by the Eastern Caribbean Central Bank or a foreign regulatory authority, by reason that it is not affiliated to any financial services group that is subject to effective consolidated supervision;

2. Introduction

The purpose of the Manual is to lay down the Company's internal practice, measures, procedures and controls relevant to the prevention of Money Laundering and Terrorist Financing. The Manual is developed and periodically updated by the Compliance Officer (hereinafter the "CO") based on the general principles set up by the Company's Board of Directors (hereinafter the "Board") in relation to the prevention of Money Laundering and Terrorist Financing.

All amendments and/or changes of the Manual shall be approved by the Board and the Senior Management. The Manual shall be communicated by the CO 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.

3. Manual Applicability

This policy applies to all company officers, employees, appointed contractors, agents, products and services offered by the Company. All business units within the company will cooperate to create a cohesive effort in the fight against money laundering. Each business unit has implemented risk-based procedures reasonably expected to detect and prevent the reporting of transactions. All efforts exerted will be documented and retained.

The CO is responsible for initiating Suspicious Activity Reports ("SARs") or other required reporting to the appropriate law enforcement or regulatory agencies. Any contacts by law enforcement or regulatory agencies related to the Policy shall be directed to the AML Compliance Officer. In this respect, the CO shall be responsible to update the Manual sin accordance with the applicable future requirements, as applicable, regarding the Client identification and due diligence procedures which the Company must follow, for Clients who deal in foreign exchange trading transactions with the Company.

All employees who are involved with investor services and cash management have been made aware of the firm's policies and procedures relating to anti-money laundering and are aware of the consequences if the firm is not in compliance with the applicable anti-money laundering legislation and regulations.

The senior level staff within the firm will continually monitor the applicable laws and regulations and will update the manuals should new regulations or laws be issued or if the firm becomes aware that we are not in compliance with the existing laws and regulations.

The Anti Money Laundering Compliance Program is designed to prevent the firm from forming business relationships or from carrying out one-off transactions with or for another person or client unless the firm can:

(a) Clearly establish the identity of the person or client;

(b) Maintain record keeping procedures in accordance with applicable laws and regulations;

4. The Responsibilities of the Board of Directors

4.1 General

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

(a) to determine, record and approve the general policy principles of the Company in relation to the prevention of Money Laundering and Terrorist Financing and communicate them to the CO

(b) 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, AML Officer and Alternative AML Compliance Officer, assistant COs and determine their duties and responsibilities, which are recorded in this Manual

(c) to approve the Manual

(d) to ensure that all relevant requirements of the Laws and Regulations are applied, and assure that appropriate, effective and sufficient systems and controls are introduced for achieving the abovementioned requirement

(e) to ensure that the CO, his assistants, if any, and any other person who has been assigned with the duty of implementing the procedures for the prevention 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

(f) 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 Money Laundering and Terrorist Financing

(g) to establish a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the CO, either directly or through his assistants, if any, and notifies accordingly the CO for its explicit prescription in the Manual

(h) to ensure that the CO and the Head of Administration/Back Office Department have sufficient resources, including competent staff and technological equipment, for the effective discharge of their duties

(i) to assess and approve the CO's Annual Report of Section 7 of the Manual and take all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the abovementioned report

(j) 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.

(k) to implement adequate and appropriate systems and processes to detect, prevent and deter money laundering arising from serious tax offences.

(l) to ensure that the Company's officials do not knowingly aid or abet Clients in committing tax offences.

(m) approve the mandatory annual training programme prepared by the CO,

(n) ensure that it receives adequate management information on the implementation of the company's AML/CFT training programme,

(o) ensure to be adequately trained to be well aware and up-to-date with the regulatory framework and the relevant responsibilities deriving from this.

5. Obligations of the Internal Auditor

5.1 General

Depending on the size and nature of the activities of the Company, an independent Internal Audit function should be established for the verification of policies, controls and procedures. Moneta Markets Ltd. may establish an internal audit function to test its anti-money laundering and financing of terrorism procedures and systems. The following obligations of the Internal Auditor are addressed specifically for the prevention of Money Laundering and Terrorist Financing:

(a) the Internal Auditor, where applicable, shall review and evaluate, at least on an annual basis, the appropriateness, effectiveness and adequacy of the policy, practices, measures, procedures and control mechanisms applied for the prevention of Money Laundering and Terrorist Financing mentioned in the Manual

(b) the findings and observations of the Internal Auditor, where applicable, in relation to point (a) above, shall be submitted, in a written report form, to the Board.

6. Money Laundering Compliance Officer

The CO shall belong hierarchically to the higher ranks of the Company's organizational structure so as to command the necessary authority. The CO shall lead the Company's Money Laundering Compliance procedures and processes and report to the Senior Management. The CO shall also have the resources, expertise as well as access to all relevant information necessary to perform his duties adequately and efficiently.

The Company shall:

(a) appoint a compliance and reporting officer who shall be responsible for ensuring the company's compliance with the provisions of the Act;

(b) the compliance and reporting officer appointed pursuant to this section will:

i. be a senior officer with the necessary qualifications and experience and able to respond adequately to enquiries relating to the company and the conduct of its business;

ii. be responsible for establishing and maintaining such a manual of compliance

iii. be responsible for ensuring that company's staff comply with the provisions of the Act and any other law relating to money laundering or financing of terrorism and the provisions of any manual of compliance procedures established; and

iv. act as the liaison officer between the company and the supervising authority and the FIU in matters relating to compliance with the provisions the Act and any other law with respect to money laundering or financing of terrorism;

v. the compliance officer shall be responsible for establishing and maintaining procedures and systems to:

(a) implement the customer identification requirements

(b) implement record keeping and retention requirements

(c) implement the reporting obligations under applicable laws

vi. Ensure the company's officers and employees are aware of the laws relating to money laundering and financing of terrorism;

vii. ensure the company's officers, employees and agents recognize suspicious transactions, trends in money laundering and financing of terrorist activities and money laundering and financing of terrorism risks within the company's products, services and operations;

The level of remuneration of the CO shall not compromise his objectivity.

7. Annual Report of the CO

7.1 General

The Annual Report of the CO is a significant tool for assessing the Company's level of compliance with its obligation laid down in the Laws and Regulations.

The CO's Annual Report shall be prepared and be submitted to the Board for approval within two months from the end of each calendar year (i.e. the latest, by the end of February each year).

Following the Board's approval of the Annual Report, a copy of the Annual Report should be submitted to the Financial Intelligence Unit on or before March 31st of each calendar year.

It is provided that the said minutes should include the measures decided for the correction of any weaknesses and/or deficiencies identified in the Annual Report and the implementation timeframe of these measures.

The Annual Report deals with issues relating to money laundering and terrorist financing during the year under review and includes, inter alia, the following:

(a) information for measures taken and/or procedures introduced for compliance with any amendments and/or new provisions of the Law and Regulations which took place during the year under review

(b) information on the inspections and reviews performed by the CO, reporting the material deficiencies and weaknesses identified in the policy, practices, measures, procedures and controls that the Company applies for the prevention of Money Laundering and Terrorist Financing. In this respect, the report outlines the seriousness of the deficiencies and weaknesses, the risk implications and the actions taken and/or recommendations made for rectifying the situation

(c) the number of Internal Suspicion Reports submitted by Company personnel to the CO, and possible comments/observations thereon

(d) the number of reports submitted by the CO to the Unit, with information/details on the main reasons for suspicion and highlights of any particular trends

(e) information, details or observations regarding the communication with the employees on money laundering and terrorist financing preventive issues

(f) information on the policy, measures, practices, procedures and controls applied by the Company in relation to high-risk Clients as well as the number and country of origin of high-risk Clients with whom a Business Relationship is established or an Occasional Transaction has been executed

(g) information on the systems and procedures applied by the Company for the ongoing monitoring of Client accounts and transactions, as and when applicable

(h) information on the training courses/seminars attended by the CO and any other educational material received

(i) information on training/education and any educational material provided to staff during the year, reporting, the number of courses/seminars organised, their duration, the number and the position of the employees attending, the names and qualifications of the instructors, and specifying whether the courses/seminars were developed in-house or by an external organisation or consultants

(j) results of the assessment of the adequacy and effectiveness of staff training

(k) information on the recommended next year's training program

(l) information on the structure and staffing of the department of the CO as well as recommendations and timeframe for their implementation, for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against Money Laundering and Terrorist Financing.

(m) an executive summary in respect to the key findings and weaknesses identified during the year under review.

8. Risk Based Approach

8.1 General

The Company shall apply adequate and appropriate measures, policies, controls and procedures, depending on its nature and size, by adopting a risk-based approach, in order to mitigate and effectively manage the risks of Money Laundering and Terrorist Financing so as to focus its effort in those areas where the risk of Money Laundering and Terrorist Financing appears to be comparatively higher.

The Company shall take appropriate measures to identify and assess the risks of Money Laundering and Terrorist Financing, taking into account risk factors including those relating to its Clients, countries or geographic areas, products, services, transactions or banking channels. Those measures should be proportionate to the size and nature of the Company.

The risk assessments referred above shall be documented, updated and made available to the Regulator and/or Supervisory Body.

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

(a) recognizes that the money laundering or terrorist financing threat varies across Clients, countries, services and securities

(b) allows the Board to differentiate between Clients of the Company in a way that matches the risk of their particular business
(c) allows the Board to apply its own approach in the formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics
(d) helps to produce a more cost-effective system
(e) promotes the prioritisation of effort and actions of the Company in response to the likelihood of Money Laundering and Terrorist Financing occurring through the use of the Securities Dealing and Brokerage Services provided by the Company.

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 Money Laundering and Terrorist Financing risks faced by the Company.

Such measures include:

(a) identifying and assessing the Money Laundering and Terrorist Financing risks emanating from particular Clients or types of Clients, securities, services, and geographical areas of operation of its Clients.
(b) managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls.
(c) continuously monitoring and improving the effective operation of the policies, procedures and controls.
(d) performing identification and due diligence in accordance with the Act.
(e) record keeping, in accordance with the Act.
(f) ensuring the existence of internal control, assessment and risk management in order to prevent Money Laundering and Terrorist Financing.
(g) undertaking a thorough examination of any transactions which, by their very nature, are particularly susceptible of being linked to Money Laundering or Terrorist Financing offenses, and in particular of any complex or abnormally large transactions and of all the unusual transactions occurring without obvious economic or clear legitimate reason.
(h) setting up risk management practices
(i) setting up compliance management
(j) ensuring that sufficient recruitment policy is in place and assessment of the employees' integrity.

(k) performing ongoing training of employees in the recognition and handling of transactions and activities which may be related to money laundering or terrorist financing

The Board of Directors shall assess and evaluate the risks it faces, for usage of the services provided for the purpose of money laundering or terrorist financing. The particular circumstances of the Company determine the suitable procedures and measures that need to be applied to counter and manage risks, the identification, recording and evaluation of risk that the Company faces presupposes the finding of the risk posed by the Company's Clients behaviour, the way the Client communicated with the Company and the risk posed by the services and securities provided by the Client.

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 inter alia the following:

- the scale and complexity of the services offered
- geographical spread of the services, products and Clients
- the nature (e.g. non-face-to-face) and economic profile of Clients as well as of securities 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 Company when assessing the risk of money laundering and terrorist financing shall take into account, among others, the Risk Factor Guidelines and any guidelines/guidance issued by the Financial Action Task Force (FATF).

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 adequate implementation of the policies, procedures and controls on a risk-based approach. The Internal Auditor shall be responsible for reviewing the adequate implementation of a risk-based approach by the CO, at least annually.

8.2 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 securities dealing and brokerage services for the purpose of Money Laundering or Terrorist Financing. The particular circumstances of the Company determine suitable procedures and measures that need to be applied to counter and manage risk.

In the cases where the Securities Dealing and brokerage services and the securities that the Company provides are relatively simple, involving relatively few Clients or Clients with similar characteristics, then the Company shall apply such procedures which are able to focus on those Clients who fall outside the 'norm'.

The Company shall be, at all times, in a position to demonstrate to the Regulator that the extent of measures and control procedures it applies are proportionate to the risk it faces for the use of the Securities Dealing and Brokerage Services provided, for the purpose of Money Laundering and Terrorist Financing.
The Company shall take the following indicative risk variables into consideration while it determines the risks implicated as well as the categorization of the clients:

i. The purpose of the account or the relationship
ii. The volume of assets that will be deposited by the client or the size of the transactions
iii. The regularity or the duration of the business relationship

8.3 Company Risks

The following, inter alia, are sources of risks which the Company faces with respect to Money Laundering and Terrorist Financing:

(a) Risks based on the Client's nature:
    - complexity of ownership structure of legal persons
    - companies with bearer shares
    - companies incorporated in offshore centers
    - 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
    - unwillingness of Client to provide information on the Beneficial Owners of a legal person.

(b) Risks based on the Client's behavior:
    - 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.

(c) Risks based on the Client's initial communication with the Company:

- non-face-to-face Clients
- Clients introduced by a third person.

(d) Risks based on the Company's services and securities:

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

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 Client Due Diligence Procedures in respect of Clients in line with their assessed Money Laundering and Terrorist Financing 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.

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

The Company shall prepare and maintain a Client list, which contain, inter alias, the Clients' names, account numbers, date of commencement of the business relationship and their risk classification. The respective list should be promptly updated with all new or existing Clients that the Company determined, in the light of additional information received, that fall under one of the risk categories.

In this respect, it is the duty of the CO to develop and constantly monitor and adjust the Company's policies and procedures with respect to the Client Acceptance Policy and Client Due Diligence and Identification Procedures, as well as via a random sampling exercise as regards existing Clients.

8.4 Dynamic Risk Management

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Clients' activities change as well as the services and securities provided by the Company change. The same happens to the securities and the transactions used for money laundering or terrorist financing.

In this respect, it is the duty of the CO to undertake regular reviews of the characteristics of existing Clients, new Clients, services and securities and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics or circumstances. These reviews shall be duly documented, as applicable, and form part of the Annual Money Laundering Report.

Relevant International Organisations

For the development and implementation of appropriate measures and procedures on a risk based approach, and for the implementation of Client Identification and Due Diligence Procedures, the CO and the Head of the Administration/Back Office Department shall consult data, information and reports [e.g. Clients from countries which inadequately apply Financial Action Task Force's (hereinafter "FATF"), country assessment reports] that are published in the following relevant international organisations

a. FATF - www.fatf-gafi.org
b. The UN Security Council Sanctions Committees - www.un.org/sc/committees
c. The International Monetary Fund (IMF) – www.imf.org

9. Client Acceptance policy

The Client Acceptance Policy (hereinafter 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 Administration/Back Office Department shall be assisting the CO with the implementation of the CAP, as applicable.

The Internal Auditor, where applicable, shall review and evaluate the adequate implementation of the CAP and its relevant provisions, at least annually and or when it is deemed to be necessary.

General Principles of the CAP

The General Principles of the CAP are the following:

(a) the Company shall classify Clients into various risk categories and based on the risk perception 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, according to the principles and procedures set out in this Manual.

(c) all documents and data described shall be collected before and/or during accepting a new Client

(d) no account shall be opened in anonymous or fictitious names(s)

(e) no account shall be opened unless the prospective Client is approved by:

- the Head of the Administration/Back Office Department
- the CO or a person from the Company's compliance function

Criteria for Accepting New Clients (based on their respective risk)

This Section describes the criteria for accepting new Clients based on their risk categorisation.

- Low Risk Clients

The Company may apply simplified customer due diligence measures in relation to a particular business relationship or transaction if it determines that the business relationship or the transaction presents a low degree of risk of money laundering and terrorist financing activities.

The Company shall accept Clients who are categorised as low risk Clients as long as the general principles under Section 10.1 of the Manual are followed.

Moreover, the Company shall follow the Simplified Client Identification and Due Diligence Procedures for low-risk Clients, according to section 16 of the Anti-Money Laundering Regulations 2014.

- Normal Risk Clients

The Company shall accept Clients who are categorised as normal risk Clients as long as the general principles under Section 10.2 of the Manual are followed.

- High Risk Clients

The Company shall accept Clients who are categorised as high-risk Clients as long as the general principles under Section 10.3 of the Manual are followed.

Moreover, the Company shall apply the Enhanced Client Identification and Due Diligence measures for high-risk Clients, according to Section 14 of the Anti-Money Laundering Regulations 2014 as well as apply the due diligence and identification procedures for the specific types of high-risk Clients mentioned below, as applicable.

- Not Acceptable Clients

The following list predetermines the type of Clients who are not acceptable for establishing a Business Relationship or an execution of an Occasional Transaction with the Company:

(a) Clients who fail or refuse to submit, the requisite data and information for the verification of their identity and the creation of their economic profile, without adequate justification

(b) Clients included on Sanction Lists.

(c) Shell Banks (The Company is prohibited from entering into, or continuing, a correspondent relationship with a shell bank. The Company shall take appropriate measures to ensure that it does not engage in or continue correspondent relationships with a credit institution or financial institution that is known to allow its accounts to be used by a shell bank).

- Client Categorisation Factors

This Section defines the criteria for the categorisation of Clients based on their risk. The CO shall be responsible for categorising Clients in one of the following three (3) categories based on the criteria of each category set below:

9.1. Low Risk Clients

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

(a) Client risk factors:

i. A licensed bank which is subject to the requirements of the domestic legislations to implement FATF standards and is supervised for compliance with the requirements under domestic legislations by a regulatory body;

ii. A recognized foreign bank;

iii. The Eastern Caribbean Central Bank;

iv. A public body in Saint Lucia; or

v. A legal entity, partnership or trust, the securities of which are listed on a recognized exchange in a jurisdiction that is an ordinary member of the International Organisation of Securities Commissions;

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

i. Life insurance policies for which the premium is low

ii. Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral

iii. a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme

iv. products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money)

(c) Geographical risk factors including the client's residency, establishment or registration:

i. A country which has effective system to counter the money laundering and terrorist financing activities;

ii. A country identified by credible sources as having a low level of corruption or other criminal activity such as money laundering and the production and supply of illicit drugs; and

iii. A country which, on the basis of credible sources, such as evaluations, detailed assessment reports or published follow-up reports by FATF, the IMF, the World Bank, the OECD or other international bodies or non-profit organisations

i. Has requirements to counter money laundering and terrorist financing that are consistent with the revised Recommendations of the FATF in February 2012, and updated from time to time: and

ii. Effectively implements the said Recommendations of FATF

Finally, the Company shall do monitoring on ongoing basis the transactions of low-risk Clients to ensure that there are no suspicious transactions.

9.2. Normal Risk Client Factors

The following types of Clients can be classified as normal risk Clients with respect to the Money Laundering and Terrorist Financing risk which the Company faces:

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

- Clients who are not physically present for identification purposes (non-face to face Clients)

9.3. High Risk Client Factors

The Company will, in addition to simplified due diligence measures, apply on a risk-sensitive basis enhanced client due diligence measures and enhanced ongoing monitoring in case there is a higher risk of money laundering, terrorist financing activities or other criminal conduct, or countries which do not apply or fully apply FATF Recommendations. The following is a non-exhaustive list of factors and types of evidence of potentially higher risk:

(a) Client risk factors:

i. the business relationship is conducted in unusual circumstances;
ii. Clients that are resident in geographical areas of higher risk;
iii. legal persons or arrangements that are personal asset-holding vehicles;
iv. companies that have nominee shareholders or shares in bearer form;
v. businesses that are cash-intensive;
vi. the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;
vii. politically Exposed persons
viii. client is a foreign financial institution or non-bank financial institution;
ix. client is a non-profit organisation;
x. client is a professional service provider; and
xi. client is a or is associated with a high net worth individual
xii. Clients convicted for a Prescribed Offence (and already served their sentence)
xiii. unwillingness of Client to provide information on the Beneficial Owners of a legal person.
xiv. trust accounts
xv. "Clients accounts" in the name of a third person
xvi. Clients who are involved in electronic gambling/gaming activities through the internet
xvii. Clients from countries which inadequately apply FATF's recommendations
xviii. any other Clients that their nature entail a higher risk of money laundering or terrorist financing
xix. any other Client determined by the Company itself to be classified as such.

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

i. private banking;
ii. products or transactions that might favour anonymity;
iii. non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;
iv. payment received from unknown or non-associated third parties;
v. new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;
vi. payment received from unassociated third parties;
vii. service involved the provision of directorship services or nominee shareholders
viii. product or service enable significant volumes of transactions to occur rapidly;
ix. product or service has unusual complexity;

(c) Geographical risk factors:

i. countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
ii. countries identified by credible sources as having significant levels of corruption or other criminal activity;
iii. countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;
iv. Countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country;
v. Other countries identified by the reporting entity as higher-risk because of its prior experiences or other factors.

(d) Risk based on the Client's behaviour:

i. Client transactions where there is no apparent legal financial/commercial rationale
ii. situations where the origin of wealth and/or source of funds cannot be easily verified
iii. unwillingness of Clients to provide information on the Beneficial Owners of a legal person.

(e) Risk based on the Client's initial communication with the Company:

i. non-face-to-face Client
ii. Clients introduced by a third person.

(f) Risk based on the Company's services and securities:

i. services that allow payments to third persons/parties

ii. large cash deposits or withdrawals

iii. products or transactions which may favour anonymity.

The Company shall perform the Risk Scoring Matrix to all its potential Clients in order to assess the risks of money laundering and terrorist financing.

Where the Company applies enhanced due diligence, it must retain sufficient information in order to demonstrate that there is a higher degree of risk of money laundering and terrorist financing and it shall adjust the extent or type of measures it undertakes to reflect the higher risk and carry out enhanced due diligence ongoing monitoring of any business relationship or transactions in order to identify any unusual or suspicious activities or transactions.

Enhanced due diligence measures include among others:

i. obtaining senior management approval prior to the establishment of business relationship;
ii. establishing the source of wealth and source of funds involved in the business relationship or one-off transaction;
iii. seeking additional independent, reliable sources, to verify information;
iv. taking additional measures to understand the ownership and financial situation;
v. taking further steps to establish the purpose and intended nature of business relationship;
vi. increasing the monitoring of the business relationship including greater scrutiny on transactions; and
vii. applying the guidelines issued by supervisory authorities.

10. Client Identification and Due Diligence Procedures

Cases for the Application of Client Identification and Due Diligence Procedures Moneta Markets Ltd. shall ascertain, before or within a reasonable time after entering into a business relationship, the identity of a customer on the basis of any official or other identifying document and verify such identity on the basis of reliable and independent source documents, data or information or other evidence as is reasonably capable of verifying the identity of the customer when—

(a) When establishing a Business Relationship

(b) When carrying out Occasional Transaction that amounts to 10,000 USD or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked

(c) When there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction in the provision of the relevant Securities Dealing and Brokerage Services.

(d) When there are doubts about the veracity or adequacy of previously Client identification data.

(e) When there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction in the provision of the relevant Securities Dealing and Brokerage Service.

(f) When there are doubts about the veracity or adequacy of previously Client identification data.

In this respect, it is the duty of the CO to apply all the relevant Client Due Diligence Identification Procedures described in this Manual and the Company's Client Acceptance Policy, as applicable. Furthermore, the Head of Administration/Back Office Department shall also be responsible to collect and file the relevant Client identification documents, according to the recording keeping procedures described in this Manual.

The Company may apply simplified due diligence measures in respect of Client relationship in case the business relationship or transaction is categorised as a lower degree of risk. The Company should obtain sufficient information in order to identify whether a business relationship or transaction is presenting lower risk.

Client Identification and Due Diligence procedures include the following:

Private customers (natural persons):

When identifying the customers identity the Company can rely on the basis of documents, data or information obtained from a reliable and independent source or from any other source that the reporting entity has reasonable grounds to believe and can be relied upon to identify and verify the identity of the customer. If the customer is a Natural person, the following information shall be collected:

i. True name and/or names used
ii. Residence address, city code, telephone number
iii. Business address
iv. Date and Place of birth

Names should be verified by:

i. Valid Passport
ii. National ID Card

iii. current photo-card driving license

It is further noted that the Company may exercise its discretion with regards to certain jurisdictions in the case where the above-mentioned documents may not be available provided that an equivalent document is requested for the verification of the client's identity.

Exception 1: Nigeria

In the case of Nigerian clients, the Company may accept a voter's card as proof of identification provided that the said document is verified via https://voters.inecnigeria.org/ and a record is kept on the client's file on CRM for record-keeping purposes. It is further noted that the Company has mandated that the following documents shall be acceptable as proof of identity:

- Passport
- National Identification Card
- Voter's Card
- National Identification Number & birth certificate
- National Identification Number & voter's card
- Driving Licence

The below indicated documents should not be older than 3-6 months from the filing date.

The current permanent address will be verified by one of the followings:

i. Proof of a recent utility bill
i. Customer's tax identification numbers, Social Security number or Government Service and Insurance System number
ii. Bank statement
iii. Credit card monthly statement
iv. The utility bill, bank statement and credit card statement should not be older than 3 months from the filing date.

The Company may exercise its discretion with regards to the copy of the customer's tax identification numbers, Social Security number or Government Service and Insurance System number to request the document to be apostilled in the country of origin.

The document(s) should be certified by either of the following:

i. a judge;
ii. a magistrate;

iii. a notary public;
iv. a barrister-at-law;
v. a Solicitor;
vi. an attorney-at-law; or
vii. a Commissioner of Oaths.

For each account we shall also make reasonable effort, prior to the settlement of the initial transaction, to obtain the following information to the extent it is applicable to the account:

i. Occupation of customer;
ii. The customer's investment objective and other related information concerning the customer's financial situation and needs;
iii. Annual income, Assets or net worth;

Client Approvals

Approval of the Account or "new client" is subject to the following terms and conditions:

i. The Customer Account Information Form is filled in completely;
ii. Clear photocopy of a valid ID with photo of the client is obtained;
iii. Recommendation of client is provided by the Investment Agent;
iv. Sufficient background check is conducted by our compliance team

All applications are carefully examined by the compliance officer to ensure that all required information/ documents are gathered. To approve an application, the Compliance officer must verify the following:

i. The completeness of the required agreement/identification documents
ii. The correctness, authenticity and completeness of the information provided by the applicant
iii. The creditworthiness of the applicant, through a database search whenever this deems necessary
iv. The probability that the applicant is involved in illegal or criminal activities
v. And, reject all applications that do not include all the necessary information

Corporate customers:

Before establishing a business relationship, a company search and/or other commercial inquiries shall be made to ensure that the corporate/other business applicant has not been, or is not in the process of being dissolved, struck off, wound-up or terminated. In the event of doubt as to the identity of the company or

its directors, or the business or its partners, a search or inquiry with the relevant Supervising Authority/Regulatory Agency shall be made.

The following relevant documents shall be obtained in respect of corporate/other business applicants:

i. Copies of the Certificate of Registration, including Articles of Incorporation or Certificate of Partnership, as appropriate,
ii. Copies of the By-Laws and Latest General Information Sheet, which lists the names of directors/partners and principal stockholders, and secondary licenses.
iii. The originals or certified copies of any or all of the foregoing documents, where required, should be produced and submitted for verification.
iv. Sworn statement as to existence or non-existence of beneficial owners.
v. Appropriate Board of Directors' resolutions and signed application forms or account opening, identifying the authorized signatories or principal officers of the corporation authorized to trade and their authorities and specimen signatures.
vi. Board Resolution authorizing the corporation to open the account with the Company.
vii. Latest Audited Financial Statements.
viii. Where necessary, we may also require additional information about the nature of the business of clients, copies of identification documents of shareholders, directors, officers and all authorized signatories

Enhanced Customer Due Diligence

The company will perform enhanced customer due diligence -

i. where a higher risk of money laundering or terrorist financing has been identified,
ii. where through supervisory guidance a high risk of money laundering or terrorist financing has been identified;
iii. where a customer or an applicant for business is from a foreign country that has been identified by credible sources as having serious deficiencies in its anti-money laundering or counter terrorist financing regime or a prevalence of corruption;
iv. in relation to correspondent banking relationships,
v. where the customer or the applicant for business is a political exposed person; or
vi. in the event of any unusual or suspicious activity

High Risk Customers/ Politically Exposed Persons

A PEP is defined in Sec 6 of the AML Regulations as an individual entrusted with a prominent public function in the last three (3) years, and includes any immediate family member or close associate of such an individual. Both local and foreign PEPs are covered by this definition.

The company will have a risk management system in place to determine if prospective clients and prospective or existing customers are PEPs and should conduct regular searches and checks for this purpose.

Measures for identifying Politically Exposed Person

The company will search for information from reliable sources and google search. The company will also rely on public information as allowed by the Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures in determining whether persons are within the definition of „close associates" (for example, partners or joint venturers), and will conduct regular searches and checks for this purpose.

Enhanced CDD and enhanced ongoing monitoring (on a risk-sensitive basis) are required whenever a customer, or any beneficial owner of a customer, is or becomes a politically exposed person (PEP). A "customer" for this purpose includes any person entering a business relationship or undertaking a one-off transaction with the reporting entity.

Procedures when dealing with "Politically Exposed Persons"

If the customer is a high risk or politically exposed person, the company will perform the following procedures:

i. adequately identify the person and verify his or her identity as set out in this section;
ii. have appropriate risk management systems to determine whether the customer is a politically exposed person;
iii. obtain the approval of senior management before establishing a business relationship with the customer;
iv. take reasonable measures to establish the person's source of wealth and source of property and
v. put in place risk management systems to determine whether a person or beneficial owner with whom that person has a business relationship is a politically exposed person, family member or close associate;

vi. ensure that the risk management procedures contain as a component, procedures for requiring that senior management approval be obtained before establishing or continuing a business relationship with a politically exposed person or a family member or close associate;

vii. take reasonable measures to establish the source of wealth and the source of funds of a person involved in a business relationship and a beneficial owner identified as a politically exposed person or a family member or close associate; and

viii. contain as a component, monitoring of the business relationship with the politically exposed person or a family member or close associate.

KYC procedures for dealings with professional intermediaries and / or reseller clients

i. When dealing with intermediaries or third parties to undertake our obligations to introduce business, we will perform the following procedures:

ii. immediately obtain the information required

iii. ensure that copies of identification data and other relevant documentation relating to the requirements will be made available to it from the intermediary or the 'third party upon request without delay; and

iv. satisfy ourselves that the third party or intermediary is regulated and supervised for, and has measures in place to comply with, the requirements.

Procedures for cross border correspondent banking and other similar relationships—

i. adequately identify and verify the identity of the person with whom it conducts such a business relationship;

ii. gather sufficient information about the nature of the business of the person;

iii. determine from publicly available information the reputation of the person and the quality of supervision to which the person is subject;

iv. assess the person's anti-money laundering and terrorist financing controls;

v. obtain approval from senior management before establishing a new correspondent relationship;

vi. document the responsibilities of the reporting entity and the person.

vii. Where the relationship is a payable-through account, a reporting entity shall ensure that the person with whom or with which it has established the relationship—

    a. has verified the identity of and performed on-going due diligence on such of that person's customers as have direct access to accounts of the reporting entity;

b. is able to provide the relevant customer identification data upon request to the reporting entity; and
c. has a physical presence in the country under the law under which it is established unless it is a part of a group that is subject to supervision as a whole

Changes to the Customer Status and Operations

The company immediately takes all necessary actions using the identification procedures and measures to provide due diligence, in order to collect the appropriate evidence in cases of:

i. changes to the customer documentation standards, such as:
ii. change of directors/secretary;
iii. change of registered shareholders and/or actual beneficiaries;
iv. change of registered office;
v. change of trustees;
vi. change of corporate name and/or trade name;
vii. change of main trading partners and/or significant new business;
viii. a material change in the way an account is operated, such as:
ix. change of persons authorized to handle its account;
x. request for opening a new account in order to provide new investment services and/or securities;
xi. a significant transaction that appears to be unusual and/or significant than the usual type of trade and profile of the client;

Enhanced Customer Scrutiny and Rejection

Based on the risk, we will analyse any logical inconsistencies in the information or behaviour of its customers. If a potential or existing client either refuses to provide the information described in the above chapters, or appears to have intentionally provided misleading information, a new account will not be opened and, after evaluating the risks involved, will consider closing any existing account. We will also refuse any account which is determined to be “high risk” by the Compliance officer.

Trust accounts

The CO shall apply the following with respect to trust accounts:

When the Company establishes a Business Relationship or carries out an Occasional Transaction with trusts, it shall ascertain the legal substance, the name and the date of establishment of the trust and verify the

identity of the trustor, trustee and Beneficial Owners, according to the Client identification procedures prescribed in throughout this Manual. Nevertheless, the Company shall receive sufficient information about the beneficiary to ensure the company is be able to identify the beneficial owner at the time of the payment or when the beneficiary exercises his acquired rights.

Furthermore, the Company shall ascertain the nature of activities and the purpose of establishment of the trust as well as the source and origin of funds requesting the relevant extracts from the trust deed and any other relevant information from the trustees. All relevant data and information shall be recorded and kept in the Client's file.

The Company shall maintain a central register of beneficial owners of trusts. The said register must hold adequate, accurate and current information on their beneficial ownership, including the identity of:

i. the trustee,
ii. the settlor,
iii. the protector,
iv. the beneficiaries or class of beneficiaries and
v. any other natural person exercising effective control over the trust.

Verification of Customer Identity

The company has implemented an integrated multilevel electronic system of information verification provided by the Customer. This system documents and checks identification details of the Customer, keeps and controls drill through reports of all the transactions.

The following are some counter checks being done by us to verify identity of clients without face-to-face contact:

i. Telephone contact of the applicant at an independently verifiable home or business number;
ii. Submission of Income tax return, and also bank statement or any proof of income;
iii. Confirmation of address through correspondence or presentation of proof of billing address;

Above procedures should be strictly implemented when opening of accounts via telephone, internet or by mail; especially if the client is just referred by another client or any of the staff. Such requirements should ideally be done prior to executing the initial transaction. For non-residents who seek to procure transactions without face-to-face contact, documents as enumerated above issued by foreign authorities must be submitted.

The company always requires its clients to submit information particularly on the source of funds. If the client states that he/she has a business, some proof of the business documents, like by-laws, Business registration, etc. are requested. Company search on the website for registered companies is done to ensure that the corporate or other business applicant is an existing business entity.

Customer identification and information of existing clients should be updated and/or amended at least once every two (2) years. This refers to change of residential or business address, new identification cards, new passport, additional business information, new business investment/venture, and the like. For any change of information before the said period the company requests a letter or document pertaining to the changes being made.

Bearing in mind the "Know – Your – Customer" principle, we should be in a position of no-doubt or no suspicions that the identities of our clients are questionable after careful evaluation of all identification documents submitted to us. This should be very important where the client is a non-resident and therefore more probing must be done on the purpose of the transaction and the sources of funds, especially if it involves a significant amount, except when such client is a long-established and well-known customer.

Once an account is opened for a client, particular care shall be taken in cases where instructions for transactions on behalf of said client is being made by another person or party, such person or party must be formally authorized by the client account to make such transactions on his/her behalf. The company shall require the necessary documents such as Special Power of Attorney (SPA) or duly signature-verified authorization given by clients; e.g., authorized to place an order; up to what amount; and authorized to get the withdrawal.

We shall establish whether the applicant for business relationship is acting on behalf of another person as trustee, nominee or agent. The Company shall obtain authorized evidence of the identity of such agents (the same documents needed as enumerated above) and authorized signatories, and the nature of their trustee or nominee capacity and duties.
In cases where a potential customer insists for confidentiality reasons, a numbered account may be opened.

Confidential numbered accounts should not function as anonymous accounts but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff. Whereas a numbered account can offer additional protection for the identity of the account-holder, the identity must be known to a sufficient number of staff to operate proper due diligence.

Shell companies are legal entities which have no business substance in their own right but through which financial transactions may be conducted. It is the policy of the company to always be cautious when dealing with these companies as these are often abused by money launderers.

In addition to the requirements about corporation, we shall require a Board of Directors' certification as to the purpose(s) of the owners/stockholders in acquiring the shell company. There must be satisfactory evidence of the identities of the beneficial owners bearing in mind the "Know-Your-Customer" principle.

As a policy, we do not allow named account holders to transact for non-account holders and should therefore exercise special care and vigilance. Where transactions involve significant amounts, the customer should be asked to produce competent evidence of identity including nationality, the purposes of the transaction, and the sources of the funds.
The company will document its verification, including all identifying information provided by the customer, the methods used and results of the verification.

Failure or Refusal to Submit Information for the Verification of Clients' Identity

Failure or refusal by a Client to submit, before or during the establishment of a Business Relationship or the execution of an occasional transaction, the requisite data and information for the verification of his identity and the creation of his economic profile, without adequate justification, constitutes elements that may lead to the creation of a suspicion that the Client is involved in money laundering or terrorist financing activities. In such an event, the Company shall not proceed with the establishment of the Business Relationship or the execution of the occasional transaction while at the same time the CO considers whether it is justified under the circumstances to submit a report to the Financial Intelligence Unit,

If, before or during the Business Relationship, a Client fails or refuses to submit, within a reasonable timeframe, the required verification data and information the Company and the CO shall terminate the Business Relationship and close all the accounts of the Client, taking also into account the specific

circumstances of the Client in question and the risks faced by the Company on possible money laundering and/or terrorist financing, while at the same time examine whether it is justified under the circumstances to submit a report to Financial Intelligence Unit.

Construction of an Economic Profile and General Client Identification and Due Diligence Principles

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

(a) the Company shall be satisfied that it's dealing with a real person and, for this reason, the Company shall obtain sufficient evidence of identity to verify that the person is who he claims to be. Furthermore, the Company shall verify the identity of the Beneficial Owner(s) of the Clients' accounts. In the cases of legal persons, the Company shall obtain adequate data and information so as to understand the ownership and control structure of the Client. Irrespective of the Client type (e.g. natural or legal person, sole trader or partnership), the Company shall request and obtain sufficient data and information regarding the Client business activities and the expected pattern and level of transactions. However, it is noted that no single form of identification can be fully guaranteed as genuine or representing correct identity and, consequently, the identification process will generally need to be cumulative

(b) the verification of the Clients' identification shall be based on reliable data and information issued or obtained from independent and reliable sources, meaning those data, and information that are the most difficult to be amended or obtained illicitly

(c) a person's residential and business address will be an essential part of his identity

(d) the Company will never use the same verification data or information for verifying the Client's identity and verifying its home address

(e) the data and information that are collected before or during the establishment of the Business Relationship, with the aim of constructing the Client's economic profile and, as a minimum, shall include the following:

- the purpose and the reason for requesting the establishment of a Business Relationship
- the anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments
- the Client's size of wealth and annual income and the clear description of the main business/professional activities/operations

(f) the data and information that are used for the construction of the Client-legal person's economic profile shall include, inter alia, the following:

- the name of the company
- the country of its incorporation
- the head offices address
- the names and the identification information of the Beneficial Owners
- the names and the identification information of the directors
- the names and the identification information of the authorised signatories
- financial information
- the ownership structure of the group that the Client-legal person may be a part of (country of incorporation of the parent company, subsidiary companies and associate companies, main activities and financial information).

The said data and information are recorded in a separate form designed for this purpose which is retained in the Client's file along with all other documents as well as all internal records of meetings with the respective Client. The said form is updated regularly or whenever new information emerges that needs to be added to the economic profile of the Client or alters existing information that makes up the economic profile of the Client.

(g) identical data and information with the abovementioned shall be obtained in the case of a Client-natural person, and in general, the same procedures with the abovementioned shall be followed

(h) Client transactions transmitted for execution, shall be compared and evaluated against the anticipated account's turnover, the usual turnover of the activities/operations of the Client and the data and information kept for the Client's economic profile. Significant deviations are investigated and the findings are recorded in the respective Client's file. Transactions that are not justified by the available information on the Client, are thoroughly examined so as to determine whether suspicions over money laundering or terrorist financing arise for the purposes of submitting an internal report to the CO.

For the purposes of the provisions relating to identification procedures and Client due diligence requirements, proof of identity is satisfactory if-

(a) it is reasonable possible to establish that the Client is the person he claims to be, and,

(b) the person who examines the evidence is satisfied, in accordance with the procedures followed under this manual, that the Client is actually the person he claims to be.

The construction of the Client's economic profile according to the provisions above shall be undertaken by the CO. In this respect, the data and information collected for the construction of the economic profile shall be fully documented and filed, as applicable, by the Head of the

Administration/Back Office Department.

Further Obligations for Client Identifications and Due Diligence Procedures

In addition to the principles described above, the Company, and specifically the CO shall:

(a) ensure that the Client identification records remain completely updated with all relevant identification data and information throughout the Business Relationship

(b) examine and check, on a regular basis, the validity and adequacy of the Client identification data and information that he maintains, especially those concerning high risk Clients.

Despite the obligation described above and while taking into consideration the level of risk, if at any time during the Business Relationship, the Company becomes aware that reliable or adequate data and information are missing from the identity and the economic profile of the Client, then the Company takes all necessary action, by applying the Client identification and due diligence procedures according to the Manual, to collect the missing data and information, the soonest possible, so as to identify the Client and update and complete the Client's economic profile.

If, during the Business Relationship, a Client fails or refuses to submit, within a reasonable timeframe the required verification data and information, the Company shall terminate the Business Relationship and closes all the accounts of the Client while at the same time shall examine whether it is justified under the circumstances to submit a report to the Financial Intelligence Unit,

In addition, the Company shall check the adequacy of the data and information of the Client's identity and economic profile, whenever one of the following events or incidents occurs:

(a) an important transaction takes place which appears to be unusual and/or significant compared to the normal pattern of transactions and the economic profile of the Client

(b) a material change in the Client's legal status and situation, such as:

   i. change of directors/secretary

   ii. change of registered shareholders and/or Beneficial Owners

iii. change of registered office
iv. change of trustees
v. change of corporate name and/or trading name
vi. change of the principal trading partners and/or undertaking of major new business activities

(c) a material change in the way and the rules the Client's account operates, such as:
i. change in the persons that are authorised to operate the account
ii. application for the opening of a new account for the provision of new investment services and/or securities.

In addition to the above, the Company, when making transfers of money between Clients' accounts, shall apply the following procedures, as applicable:

(a) Ask, from both Clients directly involved (originator of the transfer and recipient of the transfer), to complete a form of order and acceptance of the money transfer between the Clients' accounts.
(b) Before performing the money transfer, the responsible, for this purpose, person (e.g. Head of the Accounting Department) shall confirm the order and acceptance of the money transfer by telephone or by other equivalent method. If the confirmation is made by telephone, the telephone communication shall be recorded.
(c) The CO shall:
i. verify the authenticity of the signatures on the aforementioned form
ii. record (e.g., on the form) the reasons and confirm the legality of the purpose for which the transfer of money is made
iii. keep/file all records and information related to this purpose in the involved Clients' files.

Simplified Client Identification and Due Diligence Procedures

In accordance to the Act, the following simplified Client Identification and Due Diligence Procedures shall apply:

i. The Company may apply simplified Client due diligence measures if previously satisfied that the business relationship or transaction has a lower degree of risk.
ii. The Company shall be adequately monitoring the relevant transactions and the business relationship, so that unusual or suspicious transactions can be traced.
iii. When assessing the risks of Money Laundering and Terrorist Financing related to Client categories, geographic areas and to specific products, services, transactions or delivery/service channels, the

Company shall take into account at least the factors relating to the situations of potentially lower risk.

Client Identification and Due Diligence Procedures (Specific Cases)

The CO shall ensure that the appropriate documents and information with respect to the following cases shall be duly obtained, as applicable and appropriate:

Natural persons residing in the Republic

The Company shall obtain the following information to ascertain the true identity of the natural persons residing in the Republic:

(a) true name and/or names used as these are stated on the official identity card or passport
(b) full permanent address in the Republic,
(c) telephone (home and mobile) and fax numbers
(d) e-mail address, if any
(e) date and place of birth
(f) nationality and
(g) details of the profession and other occupations of the Client including the name of employer/business organisation.

It is provided that, the Company shall be able to prove that the said document is issued by an independent and reliable source. In this respect, the CO shall be responsible to evaluate the independence and reliability of the source and shall duly document and file the relevant data and information used for the evaluation, as applicable.

The Client's permanent address shall be verified using one of the following ways:

(a) visit at the place of residence (in such a case, the Company employee who carries out the visit prepares a memo which is retained in the Client's file), and
(b) the production of a recent (3-6 months) utility bill, local authority tax bill or a bank statement or any other document same with the aforesaid.

In addition to the above, the procedure for the verification of a client's identity is reinforced if the said Client is introduced by a reliable staff member of the Company, or by another existing reliable Client who is personally known to a member of the Board. Details of such introductions are kept in the Client's file.

In addition to the above, the Company shall require and receive information on public positions which the prospective Client holds or held in the last twelve (12) months as well as whether he is a close relative or associate of such individual, in order to verify if the Client is a PEP.

Joint accounts

In the cases of joint accounts of two or more persons, the identity of all individuals that hold or have the right to manage the account, are verified according to the procedures set in for individuals Sections above.

Accounts of unions, societies, clubs, provident funds and charities

In the case of accounts in the name of unions, societies, provident funds and charities, the Company ascertains their purpose of operation and verifies their legitimacy by requesting the production of the articles and memorandum of association/procedure rules and registration documents with the competent governmental authorities (in case the law requires such registration).

Furthermore, the Company shall obtain a list of the members of board of directors/management committee of the abovementioned organisations and verifies the identity of all individuals that have been authorised to manage the account according to the procedures set individuals Sections above

Accounts of unincorporated businesses, partnerships and other persons with no legal substance

In the case of unincorporated businesses, partnerships and other persons with no legal substance, the identity of the directors, partners, Beneficial Owners and other individuals who are authorised to manage the account shall be verified according to the procedures set in individuals Sections above.

In addition, in the case of partnerships, the original or a certified true copy of the partnership's registration certificate shall be obtained.

The Company shall obtain documentary evidence of the head office address of the business, ascertains the nature and size of its activities and receives all the information required according to Section for the creation of the economic profile of the business.

The Company shall request, in cases where exists, the formal partnership agreement and shall also obtain mandate from the partnership authorising the opening of the account and confirming authority to a specific person who will be responsible for its operation.

11. On-Going Monitoring Process

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 Money Laundering and Terrorist Financing.
In this respect, the CO shall be responsible for maintaining as well as developing the on-going monitoring process of the Company. The Internal Auditor shall review the Company's procedures with respect to the on-going monitoring process, at least annually.

The CO implements a Risk based approach for the on-going monitoring procedures of the Company, which is based on, inter alia, the Clients' risk categorisation and the volume of transactions estimated in the pre-account information provided. Relevant employees perform reviews of Clients' transactions at least once a week, or otherwise if requested by the CO, and reports to the CO their finding for the purposes of the on-going monitoring of the Company. The responsible employee shall also provide daily records of Clients' incoming and outgoing money transfers, to the CO.

The CO monitors and ensures, on a frequent basis, that the actual amount of funds deposited by Clients is consistent with the amount of funds indicated during the Client account opening stage, as well as with the economic profile of the Client. Additionally, all employees must be alert to detect and report internally any activity on the Client's account or behaviour, which is inconsistent with the previously disclosed/obtained information. Employees must inform accordingly the CO.

Procedures

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

(a) 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 head of the department providing the relevant securities dealing and brokerage service or any other person who identified the unusual or suspicious transactions as well as the Head of the Administration/BackOffice Department shall be responsible to communicate with the CO

(b) further to point (a) 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

(c) the ascertainment of the source and origin of the funds credited to accounts

(d) 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 tax offences.

(e) the use of appropriate and proportionate IT systems, including:

- adequate automated electronic management information systems which will be capable of supplying the Board of Directors 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 money laundering or terrorist financing 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.

(f) The monitoring of accounts and transactions shall be carried out in relation to specific types of transactions and the economic profile, as well as by comparing periodically the actual movement of the account with the expected turnover as declared at the establishment of the business relationship. Furthermore, the monitoring covers Clients who do not have a contact with the Company as well as dormant accounts exhibiting unexpected movements

(g) the monitoring of accounts held by Clients' whose identity was verified via the use of video communication.

(h) the monitoring on ongoing basis of the transactions of low-risk Clients to ensure that there are no suspicious transactions.

12. Recognition and Reporting of Suspicious Transactions / Activities

Registration for submission of Suspicious Transactions/Activities to the Financial Intelligence Unit

Reporting of Suspicious Transactions

As a general internal control procedure, directors, officers, agents and staff of the company shall report any knowledge or suspicion of money laundering activity to the Compliance Officer. The report should be formally transmitted either in hard copy report, memoranda or note, or via electronic means (inter-office email). Use of external emails in transmitting the report is prohibited. Ensure no one else is provided a copy (including blind copies). Failure to comply with such requirement exposes the reporting personnel to breach of confidentiality in violation of the Anti-Money Laundering Act.

In line with this requirement, all personnel will be required to sign a statement on breach of confidentiality provision of the AML Act. A copy of this signed statement will be filed together with the personnel file.

After thorough evaluation and reasonable belief that there is really a basis for suspicion of money laundering, Compliance Officer shall maintain a register of all reports made to the authorities as well as all reports made by the staff of the Company relative to suspicious transactions, whether or not such were reported to the Authorities.

Notwithstanding the duties of the Compliance Officer as reporting officer, the ultimate responsibility for proper supervision, reporting and compliance with the Money Laundering Prevention Act and its implementing Rules and Regulations, shall rest with the company and its Board of Directors.

The Company, its directors and employees are not allowed to disclose to the Client or third parties the fact that information on suspicious transactions has been transmitted, is being transmitted or will be transmitted to the Unit or that there is or that an analysis of such information or suspicious transactions can be carried out in relation to money laundering or terrorist financing.

The company shall institute a system for the mandatory reporting of suspicious transactions by appointing a Compliance Officer. Reporting of covered and suspicious transactions shall be done by the Compliance Officer within five (2) working days.

No person is allowed to make any disclosure that may interfere with, or adversely affect, inquiries and inquiries conducted on the calibration of revenue or the commission of specified offenses, knowing or suspecting that the above investigations are being conducted and surveys.

Suspicious Transactions

The definition of a suspicious transaction as well as the types of suspicious transactions which may be used for Money Laundering and Terrorist Financing are almost unlimited. A suspicious transaction will often be one which is inconsistent with a client's known, legitimate business or personal activities or with the normal business of the specific account, or in general with the economic profile that the Company has created for the Client.

The Company shall ensure that it maintains adequate information and knows enough about its Clients' activities in order to recognise on time that a transaction or a series of transactions is unusual or suspicious. Examples of what might constitute suspicious transactions/activities related to Money Laundering and Terrorist Financing are listed in Appendix 3 of the Manual. The relevant list is not exhaustive nor it includes all types of transactions that may be used, nevertheless it can assist the Company and its employees (especially the CO and the Head of the Administration/Back Office Department) in recognising the main methods used for Money Laundering and Terrorist Financing.

The detection by the Company of any of the transactions contained in the said list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds, the nature and economic/business purpose of the underlying transaction, and the circumstances surrounding the particular activity.

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

- monitor on a continuous basis any changes in the Client's financial status, business activities, type of transactions etc.
- 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 which is mentioned in Appendix 3 of this Manual.

Furthermore, the CO shall perform the following activities:

- 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 Internal Suspicion Report. The said reports are archived by the CO
- 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, which is also filed in a relevant file
- if, as a result of the evaluation described above, the CO decides to disclose this information to the FIU, then he prepares a written report, which he submits to the FIU.
- if as a result of the evaluation described above, the CO decides not to disclose the relevant information to the FIU, then he fully explains the reasons for his decision on the Internal Evaluation Report.

Submission of Information to the Unit

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

a) the identity of the account holders
b) the identity of the Beneficial Owners of the account
c) the identity of the persons authorised to manage the account
d) data of the volume of funds or level of transactions flowing through the account
e) connected accounts
f) in relation to specific transactions:
    - the origin of the funds
    - the type and amount of the currency involved in the transaction
    - the form in which the funds were placed or withdrawn, for example cash, cheques, wire transfers
    - the identity of the person that gave the order for the transaction
    - the destination of the funds
    - the form of instructions and authorisation that have been given
    - the type and identifying number of any account involved in the transaction.

The company shall register or maintain a complete file on all covered and suspicious transactions that have been brought to the attention of the Compliance Officer. The register shall contain details of:

i. the date on which the report is made,
ii. the person who made the report to the Compliance Officer,
iii. Information sufficient to identify the relevant papers related to said reports.

Protection of Persons Reporting

Bona fide disclosure of information by the Company or by an employee or director of the Company does not constitute a breach of any contractual or statutory, regulatory or administrative prohibition of disclosure of information, nor implies any liability for the Company or its directors or employees, even if the circumstances did not allow them to know precisely what the main illegal activity was and regardless of whether it was actually committed Illegal activity.

Prohibition from Carrying out Suspicious Transactions before Informing the FIU

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

13. Record-Keeping Procedures

Records will be kept for all documents obtained for the purpose of customer identification (KYC policy requirements) and all data of each transaction, as well as other information related to money laundering matters in accordance with the applicable anti-money laundering laws/regulations. That includes files on suspicious activity reports, documentation of AML account monitoring, etc.

Transaction effected via the company can be reconstructed, from which the authorities will be able to compile an audit trail for suspected money laundering, when such a report is made to it. The Company can satisfy within a reasonable time any inquiry or order from the authorities as to disclosure of information, including without limitation whether a particular person is the customer or beneficial owner of transactions conducted through the Company. The following document retention periods will be followed:

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

ii With respect to closed accounts, the records on customer identification, account files and business correspondence, shall be preserved and safely stored for at least seven (7) years from the dates when they were closed.

The following records must be kept:

i Copies of the evidential material of the customer identity.

ii Any non-documentary verification methods or additional methods used to verify.

iii Relevant evidential material and details of all business relations and transactions, including documents for recording transactions in the accounting books (the form and source of funds and/or securities used by the applicant for business; the form and destination of funds paid or delivered to the applicant for business or another person on his behalf; financial transactions carried out by the Company with or for each client or counterparty of the Company.

iv Relevant documents of correspondence with the customers and other persons with whom they keep a business relation.

v Description of how the company resolved all substantive discrepancies noted.

Checking and review of the documents is done by the personnel assigned to verify the accuracy and completeness of the records maintained by the company. It is important that any material irregularity or documents lacking are noted and reported for immediate correction. Transaction documents may be retained as originals or copies, on microfilm, or in electronic form, provided that such forms are admissible in court. If the records relate to on-going investigations or transactions that have been the subject of a disclosure, they shall be retained beyond the stipulated retention period until it is confirmed that the case has been closed and terminated.

14. Employees' Obligations, Education and Training

The company provides the necessary training, as well as orientation to its Agents and Compliance Officer. The Company disseminates to the staff the new procedures and guidelines needed in combating money laundering. The officers and staff are sent to orientations, training and seminars being offered by the

regulatory bodies. The company also educates staff on the "Know Your Customer" requirements on the prevention and detection of money laundering. Staff will therefore be trained in the true identity of customers and the type of business relationship being established. The company shall determine the extent of training/orientation of its personnel with the priority being given to the Compliance Officer who would be directly exposed to situations involving money laundering activities. Scope of training is on the following:

i Provisions of the Money Laundering Prevention Act
ii The Company's AML Policy
iii The Company's Internal Supervision, Control, and Compliance Procedures
iv Updates and changes on the Money Laundering Prevention Act
v Updates and changes on Internal Supervision, Control, and Compliance Procedures

Refresher training or orientations shall be made from time to time to constantly remind key staff of their responsibilities or if there are changes in the laws and rules in money laundering. The training shall be conducted at least once per quarter at minimum.

15. Test of The AML Policy

We will hire an independent, qualified party to provide an annual independent audit of our AML policies and procedures, and the compliance with said procedures. The Company will perform written follow-up to ensure that any deficiencies noted during its annual review are addressed and corrected.

Appendix 1

INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

INFORMER'S DETAILS

Name: ..... Tel: .....

Department: ..... Fax: .....

Position: .....

CLIENT'S DETAILS

Name: .....

Address: .....

..... Date of Birth: .....

Tel: ..... Occupation: .....

Fax: ..... Details of Employer: .....

.....

Passport No.: ..... Nationality: .....

ID Card No.: ..... Other ID Details: .....

INFORMATION/SUSPICION

Brief description of activities/transaction: .....

....

Reason(s) for suspicion: .....

....

Informer's Signature Date

....

FOR CO USE

Date Received: ..... Time Received: ..... Ref.....

Reported to the Unit: Yes/No.... Date Reported: ..... Ref.....

Appendix 2

INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

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

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

INQUIRIES UNDERTAKEN (Brief Description)

.....

.....

.....

ATTACHED DOCUMENTS

.....

.....

.....

.....

CO DECISION

.....

.....

.....

FILE NUMBER.....

CO SIGNATURE DATE

....

Appendix 3

Examples of Suspicious Transactions/Activities Related to Money Laundering and Terrorist Financing

A. Money Laundering

1. Transactions with no discernible purpose or are unnecessarily complex.
2. Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the Client.
3. The transactions or the size of the transactions requested by the Client do not comply with his usual practice and business activity.
4. Large volume of transactions and/or money deposited or credited into, an account when the nature of the Client's business activities would not appear to justify such activity.
5. The Business Relationship involves only one transaction or it has a short duration.
6. There is no visible justification for a client using the services of a particular financial organisation. For example, the Client is situated far away from the particular financial organisation and in a place where he could be provided services by another financial organisation.
7. There are frequent transactions in the same securities without obvious reason and in conditions that appear unusual (churning).
8. There are frequent small purchases of particular securities by a client who settles in cash, and then the total number of the securities is sold in one transaction with settlement in cash or with the proceeds being transferred, with the Client's instructions, in an account other than his usual account.
9. Any transaction the nature, size or frequency appear to be unusual, e.g., cancellation of an order, particularly after the deposit of the consideration.
10. Transactions which are not in line with the conditions prevailing in the market, in relation, particularly, with the size of the order and the frequency.
11. The settlement of any transaction but mainly large transactions, in cash.

12. Settlement of the transaction by a third person which is different than the Client which gave the order.
13. Instructions of payment to a third person that does not seem to be related with the instructor.
14. Transfer of funds to and from countries or geographical areas which do not apply or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.
15. A Client is reluctant to provide complete information when establishes a Business Relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with financial organisations, names of its officers and directors, or information on its business location. The Client usually provides minimum or misleading information that is difficult or expensive for the financial organisation to verify.
16. A Client provides unusual or suspicious identification documents that cannot be readily verified.
17. A Client's home/business telephone is disconnected.
18. A Client that makes frequent or large transactions and has no record of past or present employment experience.
19. Difficulties or delays on the submission of the financial statements or other identification documents, of a client/legal person.
20. A Client who has been introduced by a foreign financial organisation, or by a third person whose countries or geographical areas of origin do not apply or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.
21. Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g., student, unemployed, self-employed, etc.).
22. The stated occupation of the Client is not commensurate with the level or size of the executed transactions.
23. Financial transactions from non-profit or charitable organisations for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.
24. Unexplained inconsistencies arising during the process of identifying and verifying the Client (e.g., previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address and date of birth etc).

25. Complex trust or nominee network.
26. Transactions or company structures established or working with an unneeded commercial way, e.g., companies with bearer shares or bearer securities or use of a postal box.
27. Use of general nominee documents in a way that restricts the control exercised by the company's board of directors.
28. Changes in the lifestyle of employees of the financial organisation, e.g., luxurious way of life or avoiding being out of office due to holidays.
29. Changes the performance and the behaviour of the employees of the financial organisation.

B. Terrorist Financing

1. Sources and methods

The funding of terrorist organisations is made from both legal and illegal revenue generating activities. Criminal activities generating such proceeds include kidnappings (requiring ransom), extortion (demanding "protection" money), smuggling, thefts, robbery and narcotics trafficking. Legal fund-raising methods used by terrorist groups include:

i. collection of membership dues and/or subscriptions
ii. sale of books and other publications
iii. cultural and social events
iv. donations
v. community solicitations and fund-raising appeals.

Funds obtained from illegal sources are laundered by terrorist groups by the same methods used by criminal groups. These include cash smuggling by couriers or bulk cash shipments, structured deposits to or withdrawals from bank accounts, purchases of securities, wire transfers by using "straw men", false identities, front and shell companies as well as nominees from among their close family members, friends and associates.

2. Non-profit organisations

Non–profit and charitable organisations are also used by terrorist groups as a means of raising funds and/or serving as cover for transferring funds in support of terrorist acts. The potential misuse of non-profit and charitable organisations can be made in the following ways:

i. Establishing a non-profit organisation with a specific charitable purpose but which actually exists only to channel funds to a terrorist organisation.
ii. A non-profit organisation with a legitimate humanitarian or charitable purpose is infiltrated by terrorists who divert funds collected for an ostensibly legitimate charitable purpose for the support of a terrorist group.
iii. The non-profit organisation serves as an intermediary or cover for the movement of funds on an international basis.
iv. The non-profit organisation provides administrative support to the terrorist movement.

Unusual characteristics of non-profit organisations indicating that they may be used for an unlawful purpose are the following:

i. Inconsistencies between the apparent sources and amount of funds raised or moved.
ii. A mismatch between the type and size of financial transactions and the stated purpose and activity of the non-profit organisation.
iii. A sudden increase in the frequency and amounts of financial transactions for the account of a non-profit organisation.
iv. Large and unexplained cash transactions by non-profit organisations.
v. The absence of contributions from donors located within the country of origin of the non-profit organisation.