MVE Holdings Ltd

PREVENTION OF MONEY LAUNDERING & TERRORIST FINANCING MANUAL

CONFIDENTIAL

Contents

General Definitions

"**Advisory Authority**" means the Advisory Authority for Combating Money Laundering and Terrorist Financing.

"**Beneficial Owner**" means the natural person or natural persons, who ultimately own or control the Client and/or the natural person on whose behalf a transaction or activity is being conducted.

The Beneficial Owner shall at least include:

(a) In the case of corporate entities:

i. the natural person or natural persons, who ultimately own or control a legal entity through direct or indirect ownership or control a sufficient percentage of the shares or voting rights in that legal entity, a percentage of 25% plus one share to be deemed sufficient to meet this criterion: and

ii. the natural person or natural persons, who otherwise exercise control over the management of a legal entity.

(b) In the case of legal entities, such as foundations and legal arrangements, such as trusts, which administer and distribute funds:

i. where the future beneficiaries have already been determined, the natural person(s) who is/are the beneficiary of 25% or more of the property of a legal arrangements or entity; ii. where the individuals that benefit from the legal arrangement or entity have not yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates; and

iii. the natural person or natural persons who exercise control over 10% or more of the property of a legal arrangement or entity.

iv. The essence of the beneficial ownership is precisely not ownership in the ordinary sense of the word, but rather control and exercise of dominant influence. In some instances, control and legal title may not lie in the same hands.

"**Business Relationship**" means a business, professional or commercial relationship which is connected with the professional activities of the Company and which was expected, at the time when the contact was established, to have an element of duration.

*"**Client**" means any legal or physical person aiming to conclude a Business Relationship or conduct a single transaction with the Company. Counterparties are also treated as Clients only when the Company is executing a Client order by entering into a private Over-the-Counter deal/transaction (e.g. buying and selling) directly with the Counterparty.*

"**Company**" means **MVE Holdings Ltd** which is incorporated in Marshal Islands with registration number 111641.

"Law" means the Anti-Money Laundering Act,2006

"**Manual**" means the Anti-Money Laundering and Combatting Financial Crime Manual (this manual),

according to the Law.

" **Money Laundering and Terrorist Financing**" means the money laundering offences and terrorist financing offences, referred to also the following.

Every person who (a) knows or (b) at the material time ought to have known that any kind of property constitutes proceeds from the commission of a *predicate offence*, carries out the following activities:

i. converts or transfers or removes such property, for the purpose of concealing or disguising its illicit origin or of assisting in any way any person who is involved in the commission of the predicate offence to carry out any of the above actions or acts in any other way in order to evade the legal consequences of his actions;
ii. conceals or disguises the true nature, the source, location, disposition, movement of and rights in relation to, property or ownership of this property;
iii. acquires, possesses or uses such property;
iv. participates in, associates, co-operates, conspires to commit, or attempts to commit and aids and abets and provides counselling or advice for the commission of any of the offences referred to above;
v. provides information in relation to investigations that are carried out for laundering offences for the purpose of enabling the person who acquired a benefit from the commission of a predicate offence to retain the proceeds or the control of the proceeds from the commission of the said offence; and
vi. commits an offence punishable by fourteen years' imprisonment or by a pecuniary penalty by both of these penalties in the case of (a) above and by five years'
imprisonment or by a pecuniary penalty or by both in the case of (b) above.
vii. Tax crimes

"**Occasional Transaction**" means any transaction other than a transaction carried out in the course of an established Business Relationship formed by a person acting in the course of financial or other business.

"**Other Business Activities**" includes the following trust services and company services to third parties:

i. forming companies or other legal persons;
ii. acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership or a similar position in relation to other legal persons.
iii. providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement.
iv. acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement.
v. acting as or arranging for another person to act as a nominee shareholder for another

person, and

vi. any of the services or activities specified by SIBA.

"**Politically Exposed Persons (PEPs)**" means the natural persons who are or have been entrusted with prominent public functions within EU (Domestic PEPs) or outside of the EU (Foreign PEPs) and their immediate family members or persons known to be close associates of such persons.

"**Regulated Market**" means a multilateral system managed or operated by a market operator and which brings together or facilitates the bringing together of multiple third-party buying or/and selling interests in financial instruments - in the system and in accordance with its non discretionary rules - in a way that results in a contract, in respect of the financial instruments admitted to trading under its rules or/and systems, and which is authorized and functions regularly.

"**Shell Bank**" means a credit institution or an institution engaged in equivalent activities incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

1. 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 Anti-Money Laundering Compliance Officer (hereinafter the "AMLCO") 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 must be approved by the Board.

The Manual shall be communicated by the AMLCO 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.

The Manual has been prepared to comply with the provisions of the Marshall Islands Law.

All additional regulatory requirements that may apply in different jurisdictions should also be complied with.

1.1 Application

The Manual applies to all the services offered to the Company's Clients as well as the relevant Company's dealings with its Clients, including foreign exchange trading transactions, which either do not aim to physically deliver the agreed foreign currency or are not materially settled in cash (foreign exchange spot trading), irrespective of the Client account size and frequency of trading.

In this respect, the MLCO shall be responsible to update the Manual so as to comply with FSA's future requirements, as applicable, regarding the Client identification and due diligence procedures which a CIF must follow, for Clients who deal in foreign exchange trading transactions with the Company.

2. THE RESPONSIBILITIES OF THE BOARD OF DIRECTORS

2.1. 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 AMLCO

(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 AMLCO and, where is necessary, assistant AMLCOs and determine their duties and responsibilities, which are recorded in this Manual. Only persons who shall possess the relevant certificate(s) of professional competence shall be appointed as AMLCO and assistant AMLCOs, unless an exception has been obtained.

(c) to approve the Manual

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

(e) to ensure that the AMLCO and his/ her 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 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 AMLCO, as well as his/ her assistants (if any), to whom they report, any information concerning transactions and activities for which they have knowledge or suspicion that might be related to Money Laundering and Terrorist Financing

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

(h) to ensure that the AMLCO, the assistant AMLCOs, if any and the 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 AMLCO's Annual Report stated in this 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 in the Internal Auditor's report. The minutes of the said decision of the Board and the Internal Auditor's report shall be submitted within twenty (20) days from the said meeting and no later than four (4) months after the end of the calendar year (i.e. the latest, by the end of April).

(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) 'senior management' means an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors.

3. RESPONSIBILITIES OF THE INTERNAL AUDIT FUNCTION

The following responsibilities of the Internal Audit Function are addressed specifically for the prevention of Money Laundering and Terrorist Financing:

(a) the Internal Auditor 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; and

(b) the findings and observations of the Internal Auditor be submitted in a written report form to the Board.

4. ANTI-MONEY LAUNDERING COMPLIANCE OFFICER

4.1. General

The AMLCO shall belong hierarchically to the higher ranks of the Company's organisational structure so as to command the necessary authority. Furthermore, the AMLCO shall lead the Company's Money Laundering Compliance procedures and processes and report to the Board.

The AMLCO shall also have the resources, expertise as well as access to all relevant information necessary to perform his/ her duties adequately and efficiently.

The MLCO shall also have the resources, expertise as well as access to all relevant information necessary to perform his duties adequately and efficiently.

The level of remuneration of the AMLCO shall not compromise his/ her objectivity.

In performing his/ her role the Compliance/Anti-Money Laundering Officer takes into account the nature, scale and complexity of its business, and the nature and range of investment services and activities undertaken in the course of that business.

4.2. Duties of the AMLCO

During the execution of his/ her duties and the control of the compliance of the Company with the Law and the Directive, the AMLCO shall obtain and utilise data, information and reports issued by international organisations, as these are stated in Section 6.5. of the Manual.

The duties of the AMLCO shall include, *inter alia*, the following:

(a) to design, based on the general policy principles of the Company the internal practice, measures, procedures and controls relevant to the prevention of Money Laundering and Terrorist Financing, and describe and explicitly allocate the appropriateness and the limits of responsibility of each department that is involved in the abovementioned.
It is provided that, the above include measures and procedures for the prevention of the abuse of new technologies and systems providing financial services, for the purpose of Money Laundering and Terrorist Financing (e.g. services and transactions via the internet or the telephone) as well as measures so that the risk of money laundering and terrorist financing is appropriately considered and managed in the course of daily activities of the Company with regard to the development of new products and possible changes in the Company's economic profile (e.g. penetration into new markets)

(b) to develop and establish the Client Acceptance Policy and submit it to the Board for consideration and approval

(c) to review and update the Manual as may be required from time to time, and for such updates to be communicated to the Board for their approval

(d) to monitor and assess the correct and effective implementation of the policies, the practices, measures, procedures and controls of point (a) above and in general the implementation of the Manual. In this respect, the AMLCO shall apply appropriate monitoring mechanisms (e.g. on-site visits to different departments of the Company) which will provide him with all the necessary information for assessing the level of compliance of the departments and employees of the Company with the procedures and controls which are in force. In the event that the AMLCO identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, gives appropriate guidance for corrective measures and where deems necessary informs the Board

(e) to receive information from the Company's employees which is considered to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities. The information is received in a written report form (hereinafter the "Internal Suspicion Report"), a specimen of such report is attached in Appendix 1 of the Manual (f) to evaluate and examine the information received as per point (e) above, by reference to other

relevant information and discuss the circumstances of the case with the informer and where appropriate, with the informer's superiors. The evaluation of the information of point (e) above shall be done on a report (hereinafter the "Internal Evaluation Report"), a specimen of such report is attached in Appendix 2 of the Manual

(g) if following the evaluation described in point (f) above, the AMLCO decides to notify the Financial Intelligence Unit (hereinafter the "Unit").

(h) if following the evaluation described in point (f) above, the AMLCO decides not to notify the Unit then he/ she should fully explain the reasons for such a decision on the AMLCO's Internal Evaluation Report

(i) to act as a first point of contact with the Unit, upon commencement of and during an investigation as a result of filing a report to the Unit according to point (g) above (j) to ensure the preparation and maintenance of the lists of Clients categorised following a risk based approach, which contains, among others, the names of Clients, their account number and the dates of the commencement of the Business Relationship. Moreover, the AMLCO ensures the updating of the said list with all new or existing Clients, in light of any additional information obtained

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

(l) to evaluate the systems and procedures applied by a third person on whom the Company may rely for Client identification and due diligence purposes, according to this Manual, and approves the cooperation with it

(m) to ensure that the branches and subsidiaries of the Company, if any, that operate in countries outside the EEA, have taken all necessary measures for achieving full compliance with the provisions of the Manual, in relation to Client identification, due diligence and record keeping procedures

(n) to provide advice and guidance to the employees of the Company on subjects related to money laundering and terrorist financing

(o) to acquire the knowledge and skills

(p) required for the improvement of the appropriate procedures for recognising, preventing and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing

(q) to determine whether the Company's departments and employees that need further training and education for the purpose of preventing Money Laundering and Terrorist Financing and organises appropriate training sessions/seminars. In this respect, the AMLCO prepares and applies an annual staff training program according to Section 18 of the Manual. Also, the AMLCO assesses the adequacy of the education and training provided

(r) to prepare correctly and submit timely the monthly prevention statement and provide the necessary explanation to the appropriate employees of the Company for its completion (s) to prepare the Annual Report, according to Section 4 of the Manual

(t) to respond to all requests and queries, provide all requested information and fully cooperate

(u) to maintain a registry which includes the reports of points (e), (f) and (g), and relevant statistical information (e.g. the department that submitted the internal report, date of submission to the

AMLCO, date of assessment, date of reporting to the Unit), the evaluation reports of point (d) and all the documents that verify the accomplishment of his/ her duties.

(v) to ensure the preparation and maintenance of the list of Clients included in the Panama Papers (Appendix 5).

5. ANNUAL REPORT OF THE AMLCO

5.1. General

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

The AMLCO'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 together with the Board's meeting minutes, within twenty (20) days from the end of the meeting, and no later than three (3) months from the end of each calendar year (i.e. the latest, by the end of March).

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 which took place during the year under review (b) information on the inspections and reviews performed by the AMLCO, 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 AMLCO, and possible comments/observations thereon

(d) the number of reports submitted by the AMLCO 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) summary figures, on an annualised basis, of Clients' total cash deposit in Euro and other currencies in excess of the set limit of Euro 10.000 (together with comparative figures for the previous year) as reported in the monthly prevention statement of the Manual. Any comments on material

changes observed compared with the previous year are alsoreported

(g) 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

(h) information on the systems and procedures applied by the Company for the ongoing monitoring of Client accounts and transactions

(i) information on the measures taken for the compliance of branches and subsidiaries of the Company, if any, that operate in countries outside the EEA, with the requirements of the Law in relation to Client identification, due diligence and record keeping procedures and comments/information on the level of their compliance with the said requirements

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

(k) 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

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

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

(n) information on the structure and staffing of the department of the AMLCO 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.

The Company Policy is not to accept any cash deposits or cheque deposits and also any manual deposits.

6. RISK-BASED APPROACH

6.1. General Policy

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

Further, the AMLCO shall monitor and evaluate, on an on-going basis, the effectiveness of the measures and procedures of this Manual.

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 theCompany.

Such measures include:

- identifying and assessing the Money Laundering and Terrorist Financing risks emanating from particular Clients or types of Clients, financial instruments, services, and geographical areas of operation of its Clients
- managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls
- continuous monitoring and improvements in the effective operation of the policies, procedures and controls.
- promotes the prioritization of effort and actions of the Company in response to the likelihood of Money Laundering and Terrorist Financing occurring through the use ofthe Investment and Ancillary Services.
- allows the Board to differentiate between Clients of the Company in a way that matches the risk of their particular business and to apply its own approach in the formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics;

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

Such indicators include the following:

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

The Company shall assess and evaluate the risks it faces, for the use of the Investment and Ancillary 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 services and the financial instruments 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 that the extent of measures and control procedures it applies are proportionate to the risk it faces for the use of the Investment and

Ancillary Services, for the purpose of Money Laundering and Terrorist Financing.

6.2. Identification of Risks

The risk-based approach adopted by the Company involves the identification, recording and evaluation of the risks that have to be managed.

The Company shall assess and evaluate the risks it faces, for the use of the Investment and Ancillary 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 services and the financial instruments 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 that the extent of measures and control procedures it applies are proportionate to the risk it faces for the use of the Investment and Ancillary Services, for the purpose of Money Laundering and Terrorist Financing.

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 centres
- PEPs
- Clients engaged in transactions which involves significant amounts of cash
- Clients from high risk countries or countries known for high level of corruption or organised crime or drug trafficking
- Clients included in the leaked documents of Mossack Fonseca (Panama Papers) • Clients convicted for a Prescribed Offence (and already served theirsentence) • unwillingness of Client to provide information on the Beneficial Owners of a legal person.

(b) *Risks based on the Client's behaviour*:

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

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

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

(d) *Risks based on the Company's services and financial instruments*:

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

6.3. 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
- 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.
- 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)

In this respect, it is the duty of the AMLCO 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 of this Manual, respectively, as well as via a random sampling exercise as regards existing Clients. These actions shall be duly documented and form part of the Annual Money Laundering Report, as applicable.

6.4. 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 financial instruments provided by the Company change. The same happens to the financial instruments and the transactions used for money laundering or terrorist financing.

In this respect, it is the duty of the AMLCO to undertake regular reviews of the characteristics of existing Clients, new Clients, services and financial instruments and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics.

These reviews shall be duly documented, as applicable, and form part of the Annual Money Laundering Report.

6.5. 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 AMLCO and the 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 organizations

(a) FATF - www.fatf-gafi.org

(b) The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (hereinafter "MONEYVAL") - www.coe.int/moneyval

(c) The EU Common Foreign & Security Policy (CFSP)- eeas.europa.eu/cfsp/

(d) The UN Security Council Sanctions Committees - www.un.org/sc/committees (e) The International Money Laundering Information Network (IMOLIN) - www.imolin.org (f) The International Monetary Fund (IMF) – www.imf.org

(g) Office of Foreign Assets Control - www.treasury.gov

(h) Transparency International Corruption Perceptions Index -www.transparency.org/ (i) World Bank Group - www.worldbank.org/

7. Client Acceptance Policy

7.1 **General Principles of the CAP**:

The General Principles of the CAP are the following:

(a) the Company shall classify Clients into three 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 therelevant pre-account opening due diligence and identification measures and procedures have been conducted

(c) the verification of the identity of a new Client may be completed during the establishmentof the business relationship

(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 Back-Office

Department.

(f) No PEP account shall be opened unless the prospective Client is approved by the MLCO. **7.2. Criteria for Accepting New Clients (based on their respective risk)**

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

7.3. Low Risk Clients

The Company may apply simplified due diligence to the following types of Clients provided that there is a low risk or no suspicion for money laundering and Terrorist Financing.

(1) Customer risk factors:

(a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;

(b) public administrations or enterprises.

(c) customers that are resident in geographical areas of lower risk as set out in point(3); (2) Product, service, transaction or delivery channel risk factors:

(a) life insurance policies for which the premium is low;

(b) insurance policies for pension schemes if there is no early surrender option andthe policy cannot be used as collateral;

(c) 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;

(d) financial products or services that provide appropriately defined and limited servicesto certain types of customers, so as to increase access for financial inclusion purposes;

(e) products where the risks of money laundering and terrorist financing are managedby other factors such as purse limits or transparency of ownership (e.g. certain types ofelectronic money);

(3) Geographical risk factors:

(a) Member States;

(b) third countries having effective AML/CFT systems;

(c) third countries identified by credible sources as having a low level of corruption or other criminal activity;

(d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements. When commencing the establishment of a business relationship with a client/beneficial owner whose identity has not been yet verified, as a minimum the following are taken in consideration:

- The cumulative amount of deposited funds should not exceed €10,000, irrespective of the number of accounts;
- Deposits are accepted only from a bank account that is in the name of the customer.

The cumulative time must not exceed 90 days from initial contact (takes place the moment that the client either accepts the terms and conditions or makes his first deposit,whichever comes first. The Company must ensure that the number of clients with these criteria is low and for them in this timeframe must undergo at least one EDD.

(e) businesses that are cash intensive.

It is provided that, in cases mentioned in paragraphs (a) to (d) of this section, the Company may, not verify the identification of the client or possibly, the beneficial owner, neither collect information regarding the purpose and the intended nature of the business relationship or perform verification of the identity of the customer and the beneficial owner after the creation of business relationship or occasional transaction.

It is provided further that; the Company is obliged to exercise continuous monitoring of the business relationships mentioned in paragraphs (a) to (d) of this section according to the provisions of the paragraph (d) of section 1 of article 61 of the Law and report to the Unit circumstances relating to the conduct or attempt to conduct suspicious transactions.

It is provided that, further to the cases mentioned above, the Company has to gather sufficient information to establish if the Client qualifies as a low-risk Client. The said information shall be duly documented and filed, as applicable.

The Company shall classify Clients as Low Risk Clients, considering the Risk Categorization Policy.

Moreover, the Company shall follow the Simplified Client Identification and Due Diligence Procedures for low risk Clients, according to the CAP.

Clients who are categorized as Low Risk based on the Company's Risk Categorization Policy, will be screened by using the ID3 Global (GBG) software (hereinafter "the System") upon completing their personal details on their trading account (i.e. Profile details). If the applicant can be verified by the System, no further documentation will be required unless there is a suspicion of fraud and/or money laundering and/or terrorist financing or there are doubts about the applicant's identity. The Law also tightens the rules on simplified customer Due Diligence measures and the

decision to apply as such should be backed up by documentation as opposed to a blanket approach where customers fall into a certain category.

7.4. Normal Risk Clients

The Company shall classify Clients as Normal Risk Clients, considering the Risk Categorization Policy, any Client who does not fall under the 'low risk Clients' or 'high risk Clients' abovementioned categories respectively.

Applicants categorised as Normal Risk shall provide the Company with scanned copies of their passport, national identity card or Driving License for countries where the Identity Card is not issued with photograph included and valid.

7.5. High Risk Clients

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

(1) Customer risk factors:

(a) the business relationship is conducted in unusual circumstances.

(b) customers that are resident in geographical areas of higher risk as set out in

point(3); (c) legal persons or arrangements that are personal asset-holding vehicles.

(d) companies that have nominee shareholders or shares in bearer form.

(f) the ownership structure of the company appears unusual or excessively complexgiven the nature of the company's business.

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

(a) private banking.

(b) products or transactions that might favour anonymity.

(c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures.

(d) payment received from unknown or no associated third parties.

(e) 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.

(3) Geographical risk factors:

(a) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems.

(b) countries identified by credible sources as having significant levels of corruption or other criminal activity;

(c) countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;

(d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

The Company shall classify Clients who are resident in High-risk countries, as High-Risk Clients, considering the Risk Categorization Policy.

Moreover, the Company shall apply the Enhanced Client Identification and Due Diligence measures for high-risk Clients, according to this Manual.

Applicants classified as High Risk should provide the Company with scanned copies of their valid passport or alternatively, with two (2) types of valid identification documents, such as identity card and/or driving license and/or voter's card and/or other government issued document with photograph included, in case they do not have passport.

7.6. 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:

- 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.

• Shell Banks

• Clients included in Sanctions Lists.

• Clients convicted for a Prescribed Offence.

- Customers for whom reports of unusual or suspicious transactions are repeatedly submitted to the local Financial Information Unit (FIU).

- Customers whose activities or transactions are not consistent with the information available on them, their professional activity, their risk profiles and the origin of the funds.

- Gambling and betting companies (including companies with similar activities offered through the Internet) operating without authorization or supervision.

- Customers providing financial or insurance services without authorization or control by a supervisory authority.

7.7 CLIENT DUE DILIGENCE AND IDENTIFICATION PROCEDURES

7.7.1. Cases for the application of Client Identification and Due Diligence Procedures

The Company shall duly apply Client identification procedures and Client due diligence measures in the following cases:

(a) when establishing a Business Relationship

(b) when carrying out Occasional Transactions amounting to Euro 10,000 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 ofthe amount of the transaction

(d) when there are doubts about the veracity or adequacy of previously Clientidentification data.

Further, the MLCO shall be responsible to maintain at all times and use during the application of CDD and identification procedures template-checklists with respect to required documents and data from potential Clients, as per the regulation's requirements.

The Internal Auditor shall be responsible to review the adequate implementation of all the policies and procedures, at least annually.

The Back-Office Department shall also be responsible to collect and file the relevant Client identification documents, according to the recording keeping procedures described in Section 15 of this Manual.

7.7.2. Ways of application of Client Identification and Due Diligence Procedures

Client identification procedures and Client due diligence measures shall comprise:

(a) identifying the Client and verifying the Client's identity on the basis of documents, data or information obtained from a reliable and independentsource.

(b) identifying the beneficial owner and taking risk-based and adequate measures to verify the identity on the basis of documents, data or information obtained from a reliable and independent source so that the person carrying on in financial or other business knows who the beneficial owner is; as regards legal persons, trusts and similar legal arrangements, taking risk based and adequate measures to understand the ownership and control structure of the Client

(c) obtaining information on the purpose and intended nature of the businessrelationship

(d) conducting on-going monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the information and data in the possession of the person engaged in financial or other business in relation to the Client, the business and risk profile, including where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date. **(please see Ongoing Monitoring Procedure & Reporting of Suspicious Transaction).**

(e) Screening Clients against databases or third-party checks for adverse tax-related news.

(f) to maintain registers of customers' beneficial owners that must be accessible to law enforcement agencies.

7.7.3 Proof of Residence Requirements

- **Recent Utility Bill** (i.e. electric, water, telephone, gas) - The bill must be less than three (3) months old. Please note that a mobile phone will be accepted as a valid Proof of Residence only if the name on the bill matches the name of the registration and same for the telephone number.

- **Recent Bank Statement** - Must be less than three (3) months old.

Important: Screen shots of bank statements are only acceptable in cases where the bank account being used for proof of address is the same as the one used to fund the account.

- Recent Mortgage Statement
- Signed Lease Agreement still within term
- Bank, Investment Letter
- Domestic Passport for Russians and Ukrainians (make sure that the address ismatching the one mentioned in the registration)

NOTE that any document that has been used for proof of identity cannot also be used as proof of address – excepting the Domestic Passport mentioned above.

NOTE that all documents provided in any other language excepting English should be translated. Translation should be provided for each non-English document.

- Deed or Other Evidence of Property;
- Bill for Homeowner's or Renter's Insurance Policy (less than six (6) months old); •

Security System Bill/Statement (less than six (6) months old);

- Government-Issued Letters or Statements Establishing Current Address (less than twelve (12) months old).

For example:

- Tax Letters and notices;
- Letters or notices from government housing authorities;
- Jury duty notices;
- Voter registration notices;
- Other official government letters or notices showing customer name and address being verified.

The proof of residence must:

- Show current address
- Show name as indicated on the account application
- Be from a credible source (with a visible logo)

- Be dated within the last three (3) months

NOTE: P.O. Box as Proof of Residence is acceptable. IN case none of the above are available, the following are acceptable as other forms of Proof of Residence for the locals:

- Proof of residence from Municipality, Land registry

The Following are acceptable as other forms of Proof of Residence for non-locals:

- Valid Lease Agreement (one year) between the client and the land lord or between the company which employee our client and the land lord associated with the contract of employment or a letter from the company declaring our client employment duly signed by the company.

7.7.4 Joint Account - Documentsrequired

A joint account is made between 2 clients. Both clients should be fully verified in order to proceed with the approval.

Once we receive the internal Joint Account Application Form, we check if it is filled and signed by both clients.

- Married Couples – Proof of marriage is required
- 1st Degree Family Related – Proof such as birth certificate isrequired
- Non-related but having a joint bank account – Joint bank account statement is required and proof of relationship

In most cases, both account holders will submit the documents mentioned above for individuals. If additional documents are required, client will be contacted via email.

Corporate Account Information

- Certificate of Incorporation
- Certificate of Registered Office
- Memorandum and Articles of Association
- Certificate of Good Standing/Incumbency
- Certificate of Incumbency
- Certificate of Directors and Secretary
- Certificate of Shareholders
- A resolution of the board of directors for the opening of the account andgranting authority to those who will operate it
- Proof of Identification for Shareholder(s)/Director(s)/Secretary/UBO

- Proof of Residence for Shareholder(s)/Director(s)/Secretary/UBO

7.7.5 Transactions that Favour Anonymity

In the case of Clients' transactions via internet, phone, fax or other electronic means where the Client is not present so as to verify the authenticity of his/ her signature or that he/ she is the real owner of the account or that he/ she has been properly authorised to operate the account, the Company applies reliable methods, procedures and control mechanisms over the access to the electronic means so as to ensure that it deals with the true owner or the authorised signatory of the account.

The signature specimen of the client must be contained in an official document such as the passport or the national identity card. A signature on a credit/debit card is shall not be accepted. If the signature on the passport/ID is not the same as on other documents provided by the client or in the Profile details or on the Due Diligence Questionnaire then, the Client will have to fill in the Company's specimen of signature form. The signatures on the Specimen of Signature Form (attached as APPENDIX 1 in the CAP) and the KYC documentation provided should be identical.

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

Failure or refusal by a Client to submit, before the establishment of a Business Relationship or the execution of an occasional transaction, the requisite data and information for the verification of his/ her 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 AMLCO considers whether it is justified under the circumstances to submit a report to the Unit.

If, during the Business Relationship, a Client fails or refuses to submit, within a reasonable timeframe as per section 7.5.5 below, the required verification data and information, the Company after sending a final reminder to the client, shall consider terminating 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 Unit.

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

1. The construction of the Client's economic profile needs to include 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/ she claims to be. 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. Furthermore, the Company shall verify the identity of the Beneficial Owner(s) of the Clients' accounts, using World Check and/or GBG.

(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, such as a passport copy and/or copy of national identity card.

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

i. true name and/or names used as these are stated on the official identity card or passport
ii. full permanent address, including postal code
iii. telephone (home and mobile) numbers
iv. e-mail address, if any
v. date and place of birth
vi. nationality and
vii. details of the profession and other occupations of the Client including the name of employer/business organisation.

For Applicants not residing in the Republic, passports are always requested and if available, official national identity cards issued by the competent authorities of their country of origin.

(c) As Identification Documents vary from one country to another, in case the expiry date of the document may not be stated the Company can verify the validity through a third- party database

(d) If in doubt for the genuineness of any document (passport, identity card or any other documentary evidence), the Company must seek verification of identity from an independent and reliable source such as the Embassy or the consulate of the issuing country or a reputable credit or financial institution situated in the Client's country of residence.

(e) a person's residential/business address will be an essential part of his identity. The client must provide the Company with scanned copies of a recent (up to 6 months) utility bill or a bank statement or any government issued document similar to the above document, bearing the Applicant's full address (including the postal code) and name as stated in the Profile details.

Acceptable documents:

(f) Gas bill

(g) Water bill

(h) Electricity bill

(i) Landline telephone or internet bill

(j) Bank statement

(k) Credit card statement

(l) Tax documents (i.e. local authority tax bill valid for the current year, income tax – must be recent)

(m) Tenancy Agreement (must be recent, i.e. not older than one year and must be still valid) (n)

E-generated statements or utility bills*

(o) Regarding the e-generated statements or utility bills, such document can be accepted for low risk countries, as defined in the Risk Categorization Policy. For Applicants that are sub categorized as Medium Risk, the e-generated document can be accepted only upon confirmation of client's landline or office phone number.

(p) For Applicants living in very small villages or cities where the address does not contain street and number they are required to provide the Company with an extra document proving their residential address. The requirement for an extra document proving the Client's residential address applies for High Risk clients and also to Clients that their address on the utility bill provided to the Company does not include the postal code or street and number.

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

(r) the data and information that are collected before the establishment of theBusiness 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 aBusiness 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
- theClient's size of wealth and annual income and the clear description of the main business/professional activities/operations

(s) 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 (audited financial statements)
- 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).

To this purpose the Company will request from the client or the potential client, during the account opening procedure, to provide the following information and data for the construction of the economic profile:

- Estimated Annual Income in Euro
- Estimated Net Worth in Euro
- Source of funds
- Employment status
- Business/organization the client works and his/her title/position
- Amount of money that the client intents to deposit with the Company in Euro • Purpose and reason why the client wishes to trade with the Company
- Anticipated account turnover in Euro

Following the collection of all the aforementioned information and data, the Company will compare and assess the reasonableness of the actual volume of transactions of each client against the anticipated volume declared during the account opening procedure in order to identify any significant deviations and/or suspicious transactions and where applicable, to inform MOKAS.

The said information 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.

2. The Company shall apply each of the Client due diligence measures and identification procedures set out in point (1) above, but may determine the extent of such measures on a risk-sensitive basis depending on the type of Client, Business Relationship, product or transaction.

3. For the purposes of the provisions relating to identification procedures and Clientdue 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, that the Client is actually theperson he claims to be.

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

9. Further Obligations for Client Identification and Due Diligence Procedures

1. In addition to the principles described above, the Company shall:

(a) ensure that the Client identification records remain completely updated with allrelevant 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.

(c) The timeframe during which the regular review, examination and update of the Client identification is conducted, is as follows:

a. Low Risk Clients: Every second year
b. Normal Risk Clients: Every second year
c. High Risk Clients: Annualy

2. Despite the obligation described in point (1) (c) 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 outdated or are missing from the identity and the economic profile of the Client, then the Company takes all necessary action, to update and/or collect the missing data and information, the soonest possible, so as to update and complete the Client's economic profile.

3. In addition to the obligation of points (1) and (2) above, 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:

- 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 theClient

- 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 newbusiness activities

i. a material change in the way and the rules the Client's account operates, such as:

ii. change in the persons that are authorised to operate the account

iii. application for the opening of a new account for the provision of new investment services and/or financial instruments.

10. Simplified Client Identification and Due Diligence Procedures

With respect to the provisions of the Law for simplified Client Identification and Due Diligence Procedures, the following shall apply:

1. For simplified Client Identification and Due Diligence Procedures, the Company may not verify the identification of the client or the beneficial owner, neither collect information regarding the purpose and the intended nature of the business relationship or perform verification of the identity of the customer and the beneficial owner after the establishment of the business relationship or the execution of an occasional transaction;

2. The Company may not apply the enhance due diligence measures for a Client who may be categorised as a low risk Client. Furthermore, where the Client is categorised as a low risk Client, the verification of the identity of the Client and the Beneficial Owner may be completed during the establishment of a Business Relationship if this is necessary not to interrupt the normal conduct of business and where the risk of money laundering or terrorist financing occurring is low. In such situations these procedures shall be completed as soon as possible after the initial contact and before any transactions are conducted

3. When assessing the abovementioned information, the Company shall pay special attention to any activity of those Clients or to any type of transactions which may be regarded as particularly likely, by its nature, to be used or abused for money laundering or terrorist financing purposes.

4. The Company shall not consider that Clients or transactions referred to in point (1) above represent a low risk of money laundering or terrorist financing if there is information available to suggest that the risk of money laundering or terrorist financing may not be low.

5. With respect to public authorities or public bodies of the EEA countries, for which the provisions of point (1) of Section 10 may be applied, they must fulfil all the following criteria:

   (a) the Client has been entrusted with public functions pursuant to the Treaty on European Union, the Treaties on the Communities or Community secondary legislation

   (b) the Client's identity is publicly available, transparent and certain

   (c) the activities of the Client, as well as its accounting practices, are transparent

   (d) either the Client is accountable to a community institution or to the authorities of a member state, or appropriate check and balance procedures exist ensuring control of the Client's activity.

11. Enhanced Client Identification and Due Diligence (High Risk Clients)

11.1. General Provisions

These measures include the following:

(a) where the Client has not been physically present for identification purposes,the Company shall apply one or more of the following measures:

i. take supplementary measures to verify or certify the documents supplied, or

requiring confirmatory certification by a credit or financial institution

ii. ensure that the first payment of the operations is carried out through an account opened in the Client's name with a reliable creditinstitution

iii. Telephone contact with the customer at his home or office, on atelephone number which has been verified from independent and reliablesources;

iv. Communication via video call with the customer, provided the video recording and screen shot safeguards apply to the communication. It is provided that a customer, whose identity was verified hereunder cannot deposit an amount over €10.000 per annum;

v. Communication with the customer through at an address that the Financial Organization has previously verified from independent and reliable sources, in the form of a registered letter;

vi. Performing an electronic verification

11.2 Non-face-to-face Clients

1. The Company shall apply the following with respect to non-face-to-face Clients:

a. In situations where a customer, especially a non-resident of the Republic, requests the establishment of a Business Relationship or an Occasional Transaction by mail, telephone, or through the internet, the said identification information and documents kept by the Company in its records shall take the following form:

i. Original, or

ii. Certified true copy of the original, where the certification is made by the Company, in cases where it establishes the customer's identity itself, once the original is presented thereto, or

iii. Certified true copy of the original, where the certification is made by a competent authority or person that, pursuant to the relevant provision of the laws of their country, is responsible to certify the authenticity of documentation or information, or

iv. Collection of Identification information and documents via electronic verification using ID3 Global.

However, due to the difficulty in matching the Client with the collected identification data, the Company shall apply enhanced Client identification and due diligence measures, so as to effectively mitigate the risks associated with such Business Relationship or Occasional Transaction.

Practical procedures, which can be applied as implementation of the measures regarding non face-to-face Clients of the Company are the following:

- Direct confirmation of the prospective Client's true name, address and signature from a bank operating in his country of origin;

• Obtaining a reference letter from a third person;

• Telephone contact with the Client at his residence or office, before the establishment of a Business Relationship or the Occasional Transaction, on a telephone number which has been verified from a reliable and independent source; and

• Contact with the Client through mail at an address previously verified by theCompany from independent and reliable sources.

The provisions are also applied to companies or other legal persons requesting the establishment of a Business Relationship or an Occasional Transaction through mail, telephone or internet. The Company shall take additional measures for ensuring that the companies or other legal persons operate from the address of their main offices and carry out legitimate business activities.

11.3. "Politically Exposed Persons"

According to the general definition, PEPs are the natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons.

1. The meaning 'Politically Exposed Persons' includes the following natural persons who are or have been entrusted with prominent public functions:

(a) heads of State, heads of government, ministers and deputy or assistant

ministers (b) members of parliaments

(c) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances

(d) members of courts of auditors or of the boards of central banks

(e) ambassadors, chargais d'affaires and high-ranking officers in the armed forces

(f) members of the administrative, management or supervisory bodies of State-owned enterprises.

(g) members of the governing bodies of political parties;
(h) directors, deputy directors and members of the board or equivalent function of an international organization.

(i) Central Financial Institutions: Examples here would be the Court of Auditors and members on the boards of central banks
(j) Armed Forces: In this situation a PEP rating would typically only apply to a high-ranking officer
(k) International Sports Committees: Members of these committees may be influenced to vote on the location of major sporting events/contracts for building venues, etc., so have recently been included by FATF under their definition of a PEP
(l) Anyone who has a close business relationship or joint beneficial ownership of legal entities or legal arrangements with a PEP
(m) Anyone who has the sole beneficial ownership ofa legal entity which is known to have been set up for the benefit de facto of the PEP

(n) Parents and children of PEPs, Spouse or partner, Siblings, Uncles and aunts, even slightly indirect family members (such as in-laws) will be considered as a politically exposed person

2. Where a person has ceased to be entrusted with a prominent public function for a period of at least one year, the Company shall not be obliged to consider such a person as politically exposed.

3. None of the categories set out above shall be understood as covering middle rankingor more junior officials. 'Immediate family members' includes the following:

(a) the spouse or the person with which cohabit for at least one year

(b) the children and their spouses or the persons with which cohabit for at least one year (c) the parents.

4. 'Persons known to be close associates' includes the following:

(a) any natural person who is known to have joint Beneficial Ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in point (4) above

(b) any natural person who has sole Beneficial Ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de factoof the person referred to in point (4) above.

The Company shall apply the following with respect to the accounts of "Politically Exposed Persons":

5. The establishment of a Business Relationship or the execution of an occasional transaction with politically exposed persons may expose the Company to enhanced risks.

The Company shall pay more attention when the said person originate from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose anti money laundering laws and regulations are not equivalent with international standards. In determining whether the Applicant is a PEP, the Company shall:

- use World Check or ID3 Global Check (reliable electronic intelligence databases). • Before establishing a business relationship with a PEP, the Company will obtain adequate documentation to ascertain not only the identity of the said person but also his/her business reputation.
- In assessing the business reputation of a PEP the Company will obtain referenceletters from independent and reliable third parties such as his/her financial institution,

employer, lawyer etc.

- have Senior Management approval for establishing Business Relationships with such Clients or of the continuation of the business relationships with existing Clients which

have become PEPs.

- take adequate measures to establish the source of wealth and source of funds that are involved in the Business Relationship or transaction
- conduct enhanced on-going monitoring of the Business Relationship.

- Before establishing a Business Relationship or executing an Occasional Transactionwith a PEP, the Company shall obtain adequate documentation to ascertain not only the identity of the said person but also to assess his business reputation (e.g. reference letters from third parties);

- The Company shall create the economic profile of the Client by obtaining the information specified in the CLIENT CATEGORIZATION POLICY. The details of the expected business and nature of activities of the Client forms the basis for the future monitoring of the account. The profile shall be regularly reviewed and updated with new data and information. The Company shall be particularly cautious and most vigilant where its Clients are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks; and
- The account shall be subject to annual review in order to determine whether to allow its continuance of operation. A short report shall be prepared summarizing the results of the review by the person who is in charge of monitoring the account. The report shall be submittedfor consideration and approval to the Board and filed in the Client's personal file.

11.4. Clients from countries which inadequately apply FATF's recommendations

1. The FATF Recommendations constitute the primary internationally recognised standards for the prevention and detection of Money Laundering and Terrorist Financing.

2. The Company shall apply the following with respect to Clients from countries which inadequately apply FATF's recommendations:

   (a) exercise additional monitoring procedures and pay special attention to Business Relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or apply inadequately the aforesaid recommendations

   (b) with the aim of implementing the above, the Back-Office Department shall consult the country assessment reports prepared by the FATF (http://www.fatf-gafi.org), the other regional bodies that have been established and work on the principles of FATF [e.g. Moneyval Committee of the Council of Europe (www.coe.int/moneyval)] and the International Monetary Fund (www.imf.org), for identifying persons originating from countries with significant shortcomings and strategic deficiencies in their legal and administrative systems for the prevention of Money Laundering and Terrorist Financing.

   (c) With regard to the issue of corruption, one useful source of information is the Transparency International Corruption Perceptions Index which can be found onthe website of Transparency International at www.transparency.org.

11.5. Clients included in the leaked documents of Mossack Fonseca (Panama Papers)

Before the establishment of a business relationship or the carrying out of an occasional transaction, the Company should check whether the potential clients are mentioned in the Panama Papers1 and/or whether:

a. they maintain or maintained any relationship with the company Mossack Fonseca, either directly or with any third person acting for or representing MossackFonseca;

[1] https://panamapapers.icij.org/

b. they maintain or maintained any business relationship with customers introduced or managed by Mossack Fonseca or by any third person acting for or representing Mossack Fonseca.

If the potential client (or the Beneficial Owner) is included in the Panama Papers and/or the points 1 and/or 2 above applies, then the decision for establishing a Business Relationship or the execution of an Occasional Transaction with the Client shall be undertaken by an Executive Director of the Company. The same shall apply for the maintenance/continuation of a business relationship of an existing Client (natural or legal person) subject to this Manual.

2. Following the above, and in cases where the Company is willing to accept Clients subject to this Section of the Manual, then the Company shall follow the provisions of the Manual and perform the verification of the identity of such Clients or Beneficial Owners before the establishment of a Business Relationship or the carrying out of a transaction.

11.6. Account in names of companies whose shares are in bearer form – not accepted

11.7. Trust accounts

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

1. 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 policy;

2. 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.

11.8. 'Client accounts' in the name of a third person

The MLCO shall apply the following with respect to "Client accounts" in the name of a third person:

1. The Company may open "client accounts" (e.g. omnibus accounts) in the name of financial institutions from EEA countries or non-EU countries.

In case the Company receives a request to open "client accounts" (e.g. omnibus accounts) in the name of financial institutions originating from countries other than the EEA, then the Company shall examine such requests on a case by case basis and shall undertake additional due diligence measures on such financial institutions. Such additional measures shall include a country-profile assessment in terms of AML reputation and legislation, analysis of the AML measures applied by such financial institutions, whether the financial institution is supervised in terms of AML, analysis of the line of business and clientele type of the financial institution and any additional

measures deemed necessary during the assessment. It is stressed that the Company shall be extra vigilant on such cases.

2. In the case that the opening of a "client account" is requested by a third person acting as an auditor/accountant or an independent legal professional or a trust and company service provider situated in a country of the Company shall proceed with the opening of the account provided that the following conditions are met:

    - The third person is subject to mandatory professional registration in accordance with the relevant laws of the country of operation;

    - The third person is subject to regulation and supervision by an appropriate competent authority in the country of operation for Anti-Money Laundering and Terrorist Financing purposes;

    - The MLCO has assessed the Client identification and due diligence procedures implemented by the third person and has found them to be in line with the Law. A record of the assessment should be prepared and kept in a separate file maintained for each third person; and

    - The third person makes available to the Company all the data and documents described in this Policy/Manual.

11.9. Electronic gambling & gaming through the internet

The Company shall apply the following with respect to accounts related to electronic gambling/gaming through the internet:

- The Company may establish a Business Relationship or execute an Occasional Transaction in the names of persons who are involved in the abovementioned activities provided that these persons are licensed by a competent authority of a country of the EEA. For this purpose, the Company shall request and obtain, apart from the data and information required by the Manual, copy of the license that has been granted to the said persons by the competent supervisory/regulatory authority, the authenticity of which must be verified either directly

with the supervisory/regulatory authority or from other independent and reliable sources.

- Furthermore, the Company shall collect adequate information so as to understand the Clients' control structure and ensure that the said Clients apply adequate and appropriate systems and procedures for Client identification and due diligence for the prevention of money laundering and terrorist financing.

- In the case that the Client is a person who offers services (e.g. payment providers, software houses, card acquirers) to the persons mentioned in the first point above, then the Company shall request and obtain, apart from the data and information required by this Policy, adequate information so as to be satisfied that the services are offered only to licensed persons. Also, it will obtain information necessary to completely understand the ownership structure and the group in which the Client belongs, as well as any other information that is deemed necessary so as to establish the Client's economic profile. Additionally, the Company shall obtain the signed agreement between its Client and the company that is duly licensed for electronic gambling/gaming activities through the internet, by a competent authority of a country mentioned in the first point above.

For all the above cases, the decision for the establishment of a Business Relationship or the execution of an Occasional Transaction is taken by the MLCO of the Company. Moreover, the account of the said Client is closely monitored and subject to regular review with a view of deciding whether or not to permit the continuance of its operation. Accordingly, a report shall be prepared and submitted for consideration and approval to the Board and filed in the Client's personal file.

11.10. Client Identification and Due Diligence Procedures (Specific Cases)

The MLCO 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:

- True name and/or names used as these are stated on the official identity card or passport; • Full permanent address in the Republic, including postal code;
- Telephone (home and mobile) and fax numbers;
- Email address, if any;
- Date and place of birth;
- Nationality; and

- Details of the profession and other occupations of the Client including the name of employer/business organisation.

In order to verify the Client's identity/name the Company shall request the Client to present an original document which is issued by an independent and reliable source that carries the Client's photo (e.g. Passport, National Identity cards, Driving License etc). After the Company is satisfied for the Client's identity from the original identification document presented, it will keep copies.

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 MLCO 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:

- 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
- the production of a recent (up to 3 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.

- **Natural persons not residing in the Republi**c

The Company shall obtain the information described above to ascertain the true identity of the natural persons not residing in the Republic.

In addition, and without prejudice to the application on a risk-sensitive basis, 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.

Furthermore, passports shall always be requested from the Clients not residing in the Republic and, if available, official national identity cards issued by the competent authorities of their country of origin shall be obtained. Certified true copies of the pages containing the relevant information from the said documents shall also be obtained and kept in the Client's files.

In addition, if in doubt for the genuineness of any document (passport, national identity card or documentary evidence of address), the Company shall seek verification of identity with an Embassy or the Consulate of the issuing country or a reputable credit or financial institution situated in the Client's country of residence.

In addition to the aim of preventing Money Laundering and Terrorist Financing, the abovementioned

information is also essential for implementing the financial sanctions imposed against various persons by the United Nations and the European Union. In this respect, passport's number, issuing date and country as well as the Client's date of birth always appear on the documents obtained, so that the Company would be in the position to verify precisely whether a Client is included in the relevant list of persons subject to financial sanctions which are issued by the United Nations or the European Union based on a United Nations Security Council's Resolution and Regulation or a Common Position of the European Union's Council respectively

11.11 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 described above.

11.12 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.

11.13 Accounts of unincorporated businesses, partnerships and 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 outlined 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 for the creation of the economic profile of the business.

The Company shall request, in cases where it 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.

11.14 Accounts of legal persons

For Clients that are legal persons, the Company shall establish that the natural person appearing to act on their behalf, is appropriately authorised to do so and his identity is established and verified

according to the procedures outlined above.

The Company shall take all necessary measures for the full ascertainment of the legal person's control and ownership structure as well as ***the verification of the identity of the natural persons*** who are the Beneficial Owners and exercise control over the legal person according to the procedures outlined above.

The verification of the identification of a legal person that requests the establishment of a Business Relationship or the execution of an Occasional Transaction, comprises the ascertainment of the following:

- The registered number;
- The registered corporate name and trading name used;
- The full addresses of the registered office and the head offices;
- The telephone numbers, fax numbers and e-mail address;
- The members of the board of directors;
- The individuals that are duly authorised to operate the account and to act on behalf of the legal person;
- The Beneficial Owners of private companies and public companies that are not listed in a Regulated Market of an EEA country the registered shareholders that act as nominees of the Beneficial Owners; and
- The economic profile of the legal person.

For the verification of the identity of the legal person, the Company shall request and obtain, among others, original or certified true copies of the following documents:

- Certificate of incorporation and certificate of good standing (where available) of the legal person;
- Certificate of registered office;
- Certificate of directors and secretary;
- Certificate of registered shareholders in the case of private companies and public companies that are not listed in a Regulated Market of an EEA country Memorandum and articles of association of the legal person;
- A resolution of the board of directors of the legal person for the opening of the account and granting authority to those who will operate it;
- In the cases where the registered shareholders act as nominees of the Beneficial Owners, a copy

of the trust deed/agreement concluded between the nominee shareholder and the Beneficial Owner, by virtue of which the registration of the shares on the nominee shareholder's name on behalf of the Beneficial Owner has been agreed; and

- Documents and data for the verification of the identity of the persons that are authorised by the legal person to operate the account, as well as the registered shareholders and Beneficial Owners of the legal person.

Where deemed necessary for a better understanding of the activities, sources and uses of funds/assets of a legal person, the Company shall obtain copies of its latest audited financial statements (if available), and/or copies of its latest management accounts.

For legal persons incorporated outside the Republic, the Company requests and obtains documents similar to the above.

As an additional due diligence measure, on a risk-sensitive basis, the Company shall carry out (when deemed necessary) a search and obtain information from the records of the Registrar of Companies and Official Receiver of the Republic (for domestic companies) or from a corresponding authority in the company's (legal person's) country of incorporation (for foreign companies) and/or request information from other sources in order to establish that the applicant company (legal person) is not, nor is in the process of being dissolved or liquidated or struck off from the registry of the Registrar of Companies and Official Receiver and that it continues to be registered as an operating company in the records of the Registrar of Companies and Official Receiver of the Republic or by an appropriate authority outside the Republic.

It is pointed out that, if at any later stage any changes occur in the structure or the ownership status or to any details of the legal person, or any suspicions arise emanating from changes in the nature of the transactions performed by the legal person via its account, then it is imperative that further enquiries should be made for ascertaining the consequences of these changes on the documentation and information held by the Company for the legal person and all additional documentation and information for updating the economic profile of the legal person is collected.

In the case of a Client-legal person that requests the establishment of a Business Relationship or the execution of an Occasional Transaction and whose direct/immediate and principal shareholder is another legal person, the Company, before establishing a Business Relationship or executing an Occasional Transaction, shall verify the ownership structure and the identity of the natural persons who are the Beneficial Owners and/or control the other legal person.

Apart from verifying the identity of the Beneficial Owners, the Company shall identify the persons who have the ultimate control over the legal person's business and assets. In the cases that the ultimate control rests with the persons who have the power to manage the funds, accounts or investments of the legal person without requiring authorisation and who would be in a position to override the internal procedures of the legal person, the Company, shall verify the identity of the natural persons who exercise ultimate control as described above even if those persons have no direct or indirect interest or an interest of less than 25% in the legal person's ordinary share capital or voting rights.

In cases where the Beneficial Owner of a legal person, requesting the establishment of a Business Relationship or the execution of an Occasional Transaction, the Company shall implement the following procedure:

- The Company 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;

- 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 should be recorded and kept in the Client's file.

11.15 Investment funds, mutual funds and firms providing financial or investmentservices

The Company shall establish and maintain Business Relationships or execute Occasional Transactions with persons who carry out such services and activities which are incorporated and/or operating in countries of the EEA. Such persons must:

(a) Possess the necessary license or authorisation from a competent supervisory/regulatory authority of the country of their incorporation and operation to provide the said services; and

(b) Be subject to supervision for the prevention of Money Laundering and Terrorist Financing purposes.

In the case of the establishment of a Business Relationship or the execution of an Occasional Transaction with persons who carry out the above services and activities and which are incorporated and/or operating in a third country Company shall request and obtain, in addition to the abovementioned, in previous points, documentation and the information required by the Manual for the identification and verification of persons, including the Beneficial Owners, the following:

(a) a copy of the license or authorisation granted to the said person from a competent supervisory/regulatory authority of its country of incorporation and operation, whose authenticity should be verified either directly with the relevant supervisory/regulatory authority or from other independent and reliable sources; and

(b) adequate documentation and sufficient information in order to fully understand the control structure and management of the business activities as well as the nature of the services and activities provided by the Client.

In the case of investment funds and mutual funds the Company, apart from identifying Beneficial Owners, shall obtain information regarding their objectives and control structure, including documentation and information for the verification of the identity of investment managers, investment advisors, administrators and custodians.

11.16 Nominees or agents of third persons

The Company shall take reasonable measures to obtain adequate documents, data or information for the purpose of establishing and verifying the identity of:

(a) the nominee or the agent of the third person, and

(b) any third person on whose behalf the nominee or the agent is acting.

In addition, the Company shall obtain a copy of the authorization agreement that has been concluded between the interested parties.

11.17 Reliance on Third Persons for Client Identification and Due Diligence Purposes

The Company may rely on third persons for the implementation of client identification procedures and due diligence measures provided that:

- The third person ***makes immediately available*** all data and information, which must be certified true copies of the originals or as otherwise acceptable by current practices, that were collected in the course of applying Client identification and due diligence procedures;
- The Company applies the appropriate due diligence measures on the third person with respect to his professional registration and procedures and measures applied from the third person for the prevention of Money Laundering and Terrorist Financing, according to the provisions of the Law; and
- The ultimate responsibility for meeting those requirements of Client identification and due diligence shall remain with the Company who relies on the third person.

For the purposes of this Section, third person means credit institutions or financial institutions or auditors or accountants or tax consultants or independent legal professionals or person providing trust and company services which:

- They are subject to mandatory professional registration, recognized by law, and
- They subject to supervision regarding their compliance with the requirements of the EU Directive.

Without prejudice to the above, the customer and the beneficial owner identification data, information and documents are forwarded immediately from the following third parties after the request of persons that conduct financial or other activities, taking into consideration the degree of danger that arises from the type of the customer, the business relationship, the product or transaction:

(a) Credit institutions or financial organizations that fall under the scope of the EU directive and are active within the EEA;

(b) Any third party conducting financial activities (as per the definition) operating outside the EEA which:

- Is subject to mandatory professional registration recognized by the law; and

- Is subject to supervision with regard to its compliance with the said requirements

The Company may rely on third persons only at the outset of establishing a Business Relationship or the execution of an Occasional Transaction for the purpose of verifying the identity of their Clients. According to the degree of risk any additional data and information for the purpose of updating the Client's economic profile or for the purpose of examining unusual transactions executed through the

account, is obtained from the natural persons (directors, Beneficial Owners) who control and manage the activities of the Client and have the ultimate responsibility of decision making as regards to the management of funds and assets.

In the case where the third person is an accountant or an independent legal professional or a trust and company services provider from a country which is a member of the EEA or a third country then the Company, before accepting the Client identification data verified by the said third person, shall apply the following additional measures/procedures:

- The MLCO or the appointed person shall assess and evaluate the systems and procedures applied by the third person for the prevention of Money Laundering and Terrorist Financing, as applicable;
- As a result of the abovementioned assessment, the MLCO must be satisfied that the third person implements Client identification and due diligence systems and procedures which are in line with the requirements of the Law and the Directive;
- The MLCO shall maintain a separate file for every third person of the present paragraph, where it stores the assessment report and other relevant information (such as identification details, records of meetings, evidence of all relevant data and information); and
- The commencement of the cooperation with the third person and the acceptance of Client identification data verified by the third person is subject to approval by the MLCO.

For the purposes of this Section of this Policy/Manual, the terms financial institutions and persons engaged in financial business activities do not include currency exchange offices.

The MLCO shall be responsible for the implementation of the provisions mentioned in this Policy/ Manual.

The Internal Auditor shall be responsible to review the adequate implementation of the provisions mentioned herein, at least annually.

12. Outsourcing and the Company's responsibility

When the Company outsources critical or important operational functions or any investment services or activities, it remains at all times fully responsible for discharging all of its obligations under the Law. When outsourcing, the Company has in place arrangements to comply with the following conditions:

- Outsourcing does not result in the delegation by Senior Management of its responsibility.
- The relationship and obligation of the Company towards its clients under the Law is not altered.
- The conditions with which the Company must comply in order to be authorised are in accordance with the Law and are not undermined.
- None of the other conditions subject to which the Company's authorisation was granted is being removed or modified.

12.1 Outsourcing of critical functions

The Company ensures due skill, care and diligence is exercised when entering into, managing or terminating any arrangement for the outsourcing of critical or important operational functions or of any investment services or activities.

The Company takes adequate measures to ensure the following conditions are met:

- The service provider has the ability, capacity, and authorisation as this is required by law, to perform the outsourced functions, services or activities reliably in due care and professionally;
- The service provider shall carry out the outsourced functions, services or activities effectively, and to this end the Company shall establish methods for assessing the standard of performance of the service provider;
- The service provider shall properly supervise the carrying out of the outsourced functions, services or activities, and adequately manages the risks associated with the outsourcing, providing regular feedback to the Company;
- Appropriate action shall be taken if it appears that the service provider may not be carrying out the functions, services or activities effectively and in compliance with applicable laws and regulatory requirements;
- The Company shall retain the necessary expertise to supervise the outsourced functions, services or activities effectively and manage the risks associated with the outsourcing and supervise those functions and manage those risks;
- The service provider shall disclose to the Company any development that may have a material impact on its ability to carry out the outsourced functions, services or activities effectively and in compliance with applicable laws and regulatory requirements;
- The Company shall be able to terminate the arrangement for outsourcing where necessary without detriment to the continuity and quality of its provision of services to clients;
- The service provider shall cooperate with regulators in connection with the outsourced functions, services or activities;
- The Company, its internal auditors and the relevant competent authorities shall have effective access to data related to the outsourced activities, as well as to the business premises of the service provider.
- The service provider shall protect any confidential information relating to the Company and its clients;
- The Company and the service provider shall establish, implement and maintain a contingency plan for disaster recovery and periodic testing of backup facilities, where that is necessary having regard to the function, service or activity that has been outsourced.

The respective rights and obligations of the Company and of the service provider are clearly allocated and set out in a written agreement.

13. FATCA/CRS

13.1 FATCA Reportable Persons

Taking into consideration the newly proposed U.S. Regulations all Foreign Financial Institutions ("FFIs") will need to comply with the Foreign Account Tax Compliance Act ("FATCA"). In accordance to FATCA we as an FFI are required to disclose information in relation to our US reportable persons.

All US reportable persons will need to notify the FFI accordingly, so as to be able to comply with the FATCA regulations.

Definition of US reportable person:

- A U.S. citizen (including dual citizen)
- A U.S. resident alien for tax purposes
- A domestic partnership
- A domestic corporation
- Any estate other than a foreign

estate Any trust if:

- A court within the United States is able to exercise primary supervision over the administration of the trust, and
- One or more United States persons have the authority to control all substantial decisions of the trust
- Any other person that is not a foreign person.

The client is going through the ***declaration*** below to provide his/her agreement or not: • I

am not a U.S. citizen (including dual citizen) or resident

- My birthplace is not in the U.S.
- I do not have a current U.S. mailing or residence address (including a U.S. post office box or U.S. "in-care-of" address)
- I do not have a current U.S. telephone number
- I do not have standing instructions to transfer funds to an account maintained in the United States
- I do not have currently effective power of attorney or signatory authority granted to a person with a U.S. address
- I do not have an "in-care-of" or "hold mail" address that is the sole address for the Account Holder. The Investor needs to note that in the case of a Pre-existing Individual Account that is a Lower Value Account, an "in-care-of" address outside the United States is not to be treated

as U.S. indicia.

- I do not possess a U.S. TIN (hereafter “Tax Identification Number”).

In case the client is in agreement with the above declaration, will go through the CRS process. Otherwise the Client will be declined as the Company policy is to not accept US clients.

13.2 CRS Reportable Persons

Regulations based on the OECD Common Reporting Standard (“CRS”) require to collect and report certain information about an account holder’s tax residence. Each jurisdiction has its own rules for defining tax residence. In general, tax residence is the country/jurisdiction in which the client lives. Special circumstances may cause to be resident elsewhere or resident in more than one country/jurisdiction at the same time (dual residency). If the client is a U.S. citizen or tax resident under
U.S. law, the client will go through the Declaration here above.

If the tax residence is located outside US, we are legally obliged to pass on the information in this form and other financial information with respect to the Client’s financial accounts to the tax authorities and they may exchange this information with tax authorities of another jurisdiction or jurisdictions pursuant to intergovernmental agreements to exchange financial account information. The Client will need to fill in this form here below.

Country/Jurisdiction of tax residence		TIN	If no TIN available enter Reason A, B or C
1			
2			
3			

Please explain in the following boxes why you are unable to obtain a TIN if you selected Reason B above.

1	
2	

3	

Reason A - The country/jurisdiction where the Account Holder is resident does not issue TINs to its residents

Reason B - The Account Holder is otherwise unable to obtain a TIN or equivalent number (Please explain why you are unable to obtain a TIN in the below table if you have selected this reason)

Reason C - No TIN is required. (Note) Only select this reason if the domestic law of the relevant jurisdiction does not require the collection of the TIN issued by such jurisdiction)

14. RECORD-KEEPING PROCEDURES

14.1 General

The Back-Office Department of the Company shall maintain records of:

(a) the Client identification documents and information obtained during the Client identification and due diligence procedures, as applicable

(b) the details of all relevant records with respect to the provision of investment services to Clients

The documents/data mentioned above shall be kept for a period of at least seven (7) years, which is calculated after the execution of the transactions or the termination of the Business Relationship.

It is provided that the documents/data mentioned in points (a) and (b) above which may be relevant to on-going investigations shall be kept by the Company until the Unit confirms that the investigation has been completed and the case has been closed.

14.2 Format of Records

The Back-Office Department may retain the documents/data mentioned in Section 8 of this Manual, other than the original documents or their Certified true copies that are kept in a hard copy form, in other forms, such as electronic form, provided that the Back-Office Department shall be able to retrieve the relevant documents/data without undue delay and present them at any time, after a relevant request.

In case the Company will establish a documents/data retention policy, the Compliance Department shall ensure that the said policy shall take into consideration the requirements of the Law.

The Internal Auditor shall review the adherence of the Company to the above, at least annually.

15. ON-GOING MONITORING PROCESS

15.1. General

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

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 MLCO 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.

15.2. 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 investment and/or ancillary service or any other person who identified the unusual or suspicious transactions (e.g. the Head of the Administration/BackOffice Department) shall be responsible to communicate with the AMLCO

(b) further to point (a) above, the investigation of unusual or suspicious transactions by the AMLCO. 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 determine2 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:

i. adequate automated electronic management information systems which will be capable of supplying the Board of Directors and the AMLCO, 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

ii. 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.

iii. 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 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.

Notify customers, through their last known address, that their account has been left dormant for some period, with no financial activity or full and proper data update, and that their data must be updated and transactions must be undertaken within the specified period, provided that the notice includes a description of the consequences of noncompliance with the specified time period.

If the time period expired with no financial activity or data update, the company shall take these actions (within two working days):

- Classify the account as dormant and prohibit transactions;
- Transfer securities balances to the clearing house at the relevant market. In this case, transfer fees may be lifted as per the mechanism and procedures applicable;
- Maintain cash balances and make them available and not act upon them without instructions from the customer, or the relevant authorities;

[2] Albeit the Company is not expected to determine if clients are fully compliant with all their tax obligations globally.

- Supply customers, through their last known address, with a final account statement and clarify that no further account statements shall be sent until they contact the company for account activation;
- If the account is classified as dormant, customers can contact the Company to activate the account and make the necessary updates;
- Clients who do not wish to have the account activated, must contact the Company in order to close the account and have their available cash balance returned to the source and/or contact the relevant market concerning their securities dues, without violating the Company's right to close the account, taking into consideration the account opening agreement;
- Duplicate accounts may be accepted only for the following legitimate reasons:

  - Different base currency
  - Different leverage
  - Different trading strategy / trading different products
  - Requires clean history on account
  - Wants to carry out back testing on old account and trade on new one.

Clients should be restricted to 3 accounts up to a maximum of 5 for exceptions. Dealing should authorize any additional account only after checking trading on existing account. All accounts MUST be under the same email account and where possible client should close previous accounts not being used.

Clients are automatically turned in Dormant Account (when criteria are met) and Customer Support are informed in order to apply the above.

On-going monitoring is an essential aspect of effective KYC procedures. The Company can only effectively control and reduce the risk if it has an understanding of normal and reasonable account activity of its customers so that it has means of identifying transactions which fall outside the regular pattern of an account's activity.

Without such knowledge, it is likely to fail in its duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so. Extend of the monitoring needs to be risk-sensitive.

16. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS / ACTIVITIES TO THE UNIT

16.1. Reporting of Suspicious Transactions to the Unit

The Company, in cases where there is an attempt of executing transactions which knows or suspects that are related to money laundering or terrorist financing, reports, through the AMLCO its suspicion to the Unit in accordance.

16.2. Suspicious Indicators for ML/TF

16.2.1 Customer Due Diligence

- The customer provides the securities firm with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the customer has provided. This indicator may apply to account openings and to interaction subsequent to account opening, such as wire transfers.
- During the account opening process, the customer refuses to provide information to complete CDD/KYC (e.g. occupation, prior financial relationships, etc.).
- The customer, whether a person or entity, is reluctant to provide the securities firm with complete information about the nature and purpose of the customer's business, prior financial relationships, anticipated account activity, the entity's officers and directors or business location.
- The customer, whether a person or entity, is located in a jurisdiction that is known as a bank secrecy haven, a tax shelter, or high-risk geographic locations (e.g. narcotics producing jurisdiction).
- The customer is reluctant to meet personnel from the securities firm in person, is very secretive and/or evasive or becomes defensive when asked to provide more information.
- The customer refuses to identify a legitimate source for funds or provides the securities firm with information that is false, misleading, or substantially incorrect.
- The customer engages in frequent transactions with money services businesses.
- The customer's background, whether a person or entity, is questionable or does not meet expectations based on business activities.
- The customer has no discernable reason for using the firm's service or the firm's location (e.g. customer lacks roots to the local community or has come out of his or her way to use the firm).
- The customer refuses to provide information regarding the beneficial owners of an account opened for an entity, or provides information that is false, misleading or substantially incorrect.
- The customer's address is associated with multiple other accounts that do not appear to be related.
- The customer has a history of changing financial advisors and/or using multiple firms or banks. This indicator is heightened when the customer uses firms located in numerous jurisdictions.
- The customer is known to be experiencing extreme financial difficulties.
- The customer is, or is associated with, a PEP or senior political figure.
- The customer refuses to invest in more appropriate securities when those securities would require a more enhanced CDD/KYC procedure.

- The customer with a significant history with the securities firm abruptly liquidates all of his or her assets in order to remove wealth from the jurisdiction.
- The customer appears to be acting as a fiduciary for someone else but is reluctant to provide more information regarding for whom he or she may be acting.
- The customer is publicly known to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds or is known to associate with such persons. Sources for this information include news items or Internetsearches.
- The customer enquires as to how quickly he or she can liquidate accounts or earnings without explaining why or provides suspicious reasons for doing so.
- The customer opens an account or purchases a product without any regard to loss, commissions or other costs associated with that account or product.
- The customer has commercial or other types of relationships with risky persons or institutions.
- The customer acts through intermediaries, such as money managers or advisers, in order not to have his or her identity registered.
- The customer exhibits unusual concern with the securities firm's compliance with government reporting requirements and/or the firm's AML/CFT policies.
- The customer is reluctant to provide the securities firm with information needed to file reports or fails to proceed with a transaction once asked for documentation or learns of recordkeeping requirements.
- The customer is interested in paying higher charges to the securities firm in order to keep some of his or her information secret.
- The customer tries to persuade an employee of the securities firm not to file a required report or not to maintain required records.
- The customer funds deposits, withdraws or purchases financial or monetary instruments below a threshold amount in order to avoid any reporting or recordkeeping requirements imposed by the jurisdiction.
- The customer requests that account openings and closings in his or her name or in the name of family members be done without producing a paper trail.
- Law enforcement has issued subpoenas regarding a customer and/or account at the securities Firm.

16.2.2 Fund Transfers and/or Deposits

- Wire transfers are sent to, or originate from, financial secrecy havens, tax shelters or high risk geographic locations (e.g. jurisdictions known to produce narcotics/psychotropic drugs or to be related to terrorism) without an apparent business reason or connection to a securities

transaction.

- Wire transfers or payments to or from unrelated third parties (foreign or domestic) or where the name or account number of the beneficiary or remitter has not been supplied.
- Many small, incoming wire transfers or deposits are made, either by the customer or third parties, using cheques, money orders or cash that are almost immediately withdrawn or wired out in a manner inconsistent with customer's business or history.
- Incoming payments made by third-party cheques or cheques with multiple endorsements.
- Deposit of large amount of small-denomination currency to fund account or exchanges of small notes for bigger notes.
- Wire transfer activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.
- The securities account is used for payments or outgoing wire transfers with little or no securities activities (e.g. account appears to be used as a depository account or a conduit for transfers).
- The controlling owner or officer of a public company transfers funds into his personal account or into the account of a private company that he or she owns or that is listed as an authorized signatory.
- Quick withdrawal of funds after a very short period in the account.
- Transfer of funds to financial or banking institutions other than those from where the funds were initially directed, specifically when different countries are involved.
- Transfers/journals between different accounts owned by the customer with no apparent business purpose.
- Customer requests that certain payments be routed through Nostro or correspondent accounts held by the financial intermediary or sundry accounts instead of its own account.

16.2.3 Bearer Securities

- The customer requests cashing bearer securities without first depositing them into an account or frequently deposits bearer securities into an account.
- The customer's explanation regarding the method of acquiring the bearer securities does not make sense or changes.
- The customer deposits bearer securities together with a request to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.

16.2.4 Unusual Securities Transactions and Account Activity

- Transaction where one-party purchases securities at a high price and then sells them at a considerable loss to another party. This may be indicative of transferring value from one party

to another.

- A customer's transactions include a pattern of sustained losses. This may be indicative of transferring value from one party to another.
- The purchase and sale of non-listed securities with a large price differential within a short period of time. This may be indicative of transferring value from one party to another.
- Payments effected by administrators and asset managers in cash, bearer cheques or other transferable instruments without identifying who they are for or providing very little information regarding the underlying account holder or beneficiary.
- A company uses cash to pay dividends to investors.
- Use of shell companies to purchase public company shares, in particular if the public company is involved in a cash intensive business.
- Transfer of assets without a corresponding movement of funds, such as through journaling or effecting a change in beneficial ownership.
- A dormant account that suddenly becomes active without a plausible explanation (e.g. large cash deposits that are suddenly wired out).
- A customer's transactions have no apparent economic purpose.
- A customer who is unfamiliar with a financial product's performance and specifications but wants to invest in it nonetheless.
- Transactions that show the customer is acting on behalf of third parties.
- The purchase of long term investments followed by a liquidation of the accounts shortly thereafter, regardless of fees or penalties.
- Transactions involving an unknown counterparty.
- Large sum cash purchases of financial instruments and mutual funds holdings followed by instant redemption.

16.2.5 Activity that is Inconsistent with the Customer's Business Objective or Profile

- The customer maintains multiple accounts, or maintains accounts in the names of family members
- The customer's account is not used for its intended purpose
- The customer enters into a financial commitment that appears beyond his or her means. • The customer begins to use cash extensively.
- The customer engaged in extremely complex transactions where his or her profile would indicate otherwise.

- Customer's credit usage is in extreme amounts that do not correspond to his or her financial status or collateral, which is provided by an unrelated third-party.
- The time zone in customer's location is not consistent with the times that the trades were executed, with no apparent business or other purpose, or there is a sudden change inconsistent with the customer's typical business activity.
- A foreign based customer that uses domestic accounts to trade on foreign exchanges.
- The customer exhibits a lack of concern about higher than normal transaction costs.

16.2.6 Rogue Employees

- The employee appears to be enjoying a lavish lifestyle that inconsistent with his or her salary or position.
- The employee is reluctant to take annual leave.
- The employee is subject to intense job-related demands, such as sales or production goals that may make him more willing to engage in or overlook behavior that poses ML/TF risks.
- The employee inputs a high level of activity into one customer account even though the customer's account is relatively unimportant to the organization.
- The employee is known to be experiencing a difficult personal situation, financial or other.
- The employee has the authority to arrange and process customer affairs without supervision or involvement of colleagues.
- The management/reporting structure of the financial institution allow an employee to have a large amount of autonomy without direct control over his activities.
- The employee's location is in a different country to his direct line of management, and supervision is only carried out remotely.
- A management culture within the financial institution focuses on financial reward over compliance with regulatory requirements.
- The employee's supporting documentation for customers' accounts or orders is incomplete or missing.
- Business is experiencing a period of high staff turnover or is going through significant structural changes.

16.3 Suspicious Indicators for Predicate Offences to Money Laundering Linked to Securities

16.3.1 Insider Trading

- The customer makes a large purchase or sale of a security, or option on a security,

shortly before news is issued that affects the price of the security.

- The customer is known to have friends or family who work for the securitiesissuer. • A customer's trading patterns suggest that he or she may have inside information.

16.3.2 Market Manipulation, including Penny Stocks

- A customer engages in prearranged or other non-competitive securities trading, including wash or cross trades of illiquid or low-priced securities.
- Securities or funds transfers between parties without an apparent relationship.
- Securities transactions occur across many jurisdictions, and in particular high -risk jurisdictions.
- Two or more unrelated accounts at the securities firm trade an illiquid or low-priced security suddenly and simultaneously.
- A customer makes transfers of securities between unrelated accounts for no apparent business reason.
- A customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.
- Transactions between the same or related parties structured solely so that one side incurs a loss while the other incurs a gain.
- Transaction where one-party purchases securities at a high price and then sells them at a considerable loss to another party.
- The customer deposits a large amount of securities in physical form at the securities firm.
- The physical securities are titled differently to the name on the account.
- The physical security does not bear a restrictive legend even though the history of the stock and/or the volume of shares being traded suggest that it should have such a legend.
- The customer's explanation regarding the method of acquiring the physical securities does not make sense or changes.
- The customer deposits physical securities together with a request to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.
- Large or repeated trading in securities that are illiquid, low priced or difficult to price. • The company at issue has no apparent business, revenues or products.
- The company at issue has experienced frequent or continuous changes in its business structure and/or undergoes frequent material changes in business strategy or its line of business.
- The officers or insiders of the company at issue are associated with other low priced, illiquid or

low volume companies.

- The officers or insiders of the low priced, illiquid or low volume company have a history of regulatory violations.
- The low priced, illiquid or low volume company at issue has failed to make required regulatory disclosures.
- The low priced, illiquid or low volume company at issue has been the subject of a prior trading suspension.
- A customer's transactions include a pattern of receiving physical securities or receiving incoming shares transfers that are sold with the proceeds wire transferred out of the account.
- The purchase and sale of non-listed securities with a large price differential within a short period of time.

16.3.4 Securities Offering Fraud

- The customer opens numerous accounts for different legal entities that the customer controls.
- The customer receives many incoming cheques or wire transfers from unrelated third parties.
- The customer allocates incoming third-party deposits among numerous accounts.
- The customer makes numerous outgoing payments to third parties close in time to when the customer receives many incoming third party cheques or wire transfers.
- The customer's profile does not suggest a legitimate business reason for receiving many third party deposits.
- The cheques or wire transfers note that the funds are for an investment

16.4 Risk Based Approach (RBA)

Accordingly to the Anti-Money Laundering, company must apply a 'Risk Based Approach'; that is, an approach that not only takes into consideration regulatory and/or legislative matters such as client identification, record keeping and reporting requirements but also assess the nature of their business.

The risk based approach:

- Primary Risk: Quantitative data which encompasses key legislative and regulatory components;
- Secondary Risk: Quantitative data based on key business operations which may influence the risk exposure of the Firm.

• AML/CFT membership(s) • Passporting / Cross-border permissions

• Sanctions	• Physical Representations
• Corruption	• Language Support

When reviewing individual clients, there are three phases that are taken into consideration

Phase I

The first phase aims at establishing whether the individual is categorized as a Politically Exposed Person (hereinafter as "PEP"). In the event they are categorized as PEPs, and their net deposits have exceeded 15,000 EUR (or currency equivalent) then enhanced due diligence should be conducted.

Phase II

The second phase takes into consideration the client's country of residence and the risk level associated with the jurisdiction in accordance with Annex A.

Phase III

The third phase looks at establishing the monetary parameter (total net deposits amount) at which Enhanced Due Diligence shall be conducted based on the individuals overall risk score.

Low +200,000

Normal	**+100,000**
High	**+50,000**
PEP	**+15,000**

17.5 Reporting / Record Keeping

Applying a risk-based approach, we aim to detect unusual or suspicious activities by setting limits for a particular type or category of accounts such as:

➔ Amount of deposits

➔ Omnibus accounts

➔ Transactions based on cash deposits

➔ Type of traded product

➔ Trade in the commodity markets

➔ Delivery channel/market access point

➔ Large withdrawal amounts

➔ Over-volume transaction

➔ High Risk jurisdictions

➔ PEPs

- Transactions executed for the customer are compared and evaluated against the anticipated accounts turnover, the usual turnover of the activities/operations of the customer and the data and information kept for the customer's economic profile – quarterly;

- Also the person, who carries out the checks, must ensure that all documentation received by the client is sufficient and up to date. Any document missing must be requested from the client;
- Customers' trading accounts are checked for securities offering fraud and market manipulation on daily basis – Dealing;
- Withdrawals – should take place after the POI and POR are checked to be up to date – Finance;
- Deposits - should take place after the POI, POR are checked to be up-to-date and the annual income to match with the total amount of deposits. Please also take in the consideration the limit amounts for EDD which if are exceed should be escalated to Compliance – Finance;
- Clients possessing more than three CC Monthly Audit – Compliance;
- Duplicate accounts– to be checked monthly;
- BIs, Tied Agents and Affiliates Quarterly audit – Compliance;
- Complaints quarterly monitoring – Compliance;

Significant deviations are investigated and when a suspicious activity is recognized, further investigation is required in order to obtain explanation 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.

Besides the checks that are done on an ongoing basis by the MLCO, the personnel must report to MLCO any suspicious activity or transaction in order to be reviewed and reported further to the FIU. All the findings are recorded to a separate, dedicated folder along with clients' details. (Appendix 8)

17. AMLCO's Report to the Unit

17.1 Reporting of Suspicious Transactions to the Unit

The Company, in cases where there is an attempt of executing transactions which it knows or suspects that are related to money laundering or terrorist financing, reports, through the MLCO its suspicion to the Unit in accordance with point (g) of Section 6.2 and this section. In accordance with Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures for Reporting Entities in Seychelles, all reporting entities should submit Suspicious Activities Reports and Suspicious Transactions Reports directly to the FIU.

17.2 Suspicious Transactions

1. 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.

2. Examples of what might constitute suspicious transactions/activities related to Money Laundering and Terrorist Financing are listed in Appendix 4. 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 MLCO and the Brokerage 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.

3. In order to identify suspicious transactions, the MLCO 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 4.

Furthermore, the MLCO 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 MLCO;

- 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 MLCO 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 MLCO decides to disclose this information to the Unit, then he prepares a written report, which he submits to the Unit;
- If as a result of the evaluation described above, the MLCO decides not to disclose the relevant information to the Unit, then he fully explains the reasons for his decision on the Internal Evaluation Report.

17.3. MLCO's Report to the Unit

After the submission of a suspicion report to Unit by the MLCO, the Company may subsequently wish to terminate its relationship with the Client concerned for risk avoidance reasons. In such an event, the Company exercises particular caution, not to alert the Client concerned that a suspicion report has been submitted to the Unit. Close liaison with the Unit is, therefore, maintained in an effort to avoid any frustration to the investigations conducted.

After submitting the suspicion report, the Company adheres to any instructions given by the Unit and, in particular, as to whether or not to continue or suspend a particular transaction or to maintain the particular account active.

Furthermore, after the submission of a suspicion report, the Clients' accounts concerned as well as any other connected accounts are placed under the close monitoring of the MLCO.

17.3.1. Submission of Information to the Unit

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

- the identity of the account holders;
- the identity of the Beneficial Owners of the account;
- the identity of the persons authorised to manage the account;
- data of the volume of funds or level of transactions flowing through the account;
- connected accounts;
- in relation to specific transactions:

- the origin of the funds.

- the type and amount of the currency involved in the transaction.

- the form in which the funds were placed or withdrawn, for example cash, cheques, wire transfers.

- the identity of the person that gave the order for the transaction;

- the destination of the funds; and

- the form of instructions and authorization that have been given the type and identifying number of any account involved in the transaction.

The Company shall ensure that in the case of a suspicious transaction investigation by the Unit, the AMLCO will be able to provide without delay any required information.

18. EMPLOYEES' OBLIGATIONS, EDUCATION AND TRAINING

18.1. Employees' Obligations

(a) The Company's employees shall be personally liable for failure to report information or suspicion, regarding money laundering or terrorist financing,

(b) the employees must cooperate and report, without delay, anything that comes to their attention in relation to transactions for which there is a slight suspicion that are related to money laundering or terrorist financing,

(c) according to the Law, the Company's employees shall fulfil their legal obligation to report their suspicions regarding Money Laundering and Terrorist Financing, after their compliance with point (b) above.

18.2. Education and Training

18.2.1. Employees' Education and Training Policy

(a) The Company shall ensure that its employees are fully aware of their legal obligations according to the Law, by introducing a complete employees' education and training program (b) the timing and content of the training provided to the employees of the various departments will be determined according to the needs of the Company. The frequency of the training can vary depending on to the amendments of legal and/or regulatory requirements, employees' duties as well as any other changes in the financial system.

(c) the training program aims at educating the Company's employees on the latest developments in

the prevention ot Money Launc:1enng anc:1 ı erronst 1-mancmg, mc1uc:1mg the practical methods anc:1 trends used for this purpose

(d) the training program will have a different structure for new employees, existing employees and for different departments of the Company according to the services that they provide. On-going training shall be given at regular intervals so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any newdevelopments.

The AMLCO shall be responsible to refer to the relevant details and information in his/her Annual Report in respect of the employees' education and training program undertaken each year.

18.2.2 MLCO Education and Training Program

The *Senior Management* of the Company shall be responsible for the MLCO of the Company to attend external training. Based on his/her training, the MLCO will then provide training to the employees of the Company further to Section 13.2 above.

The main purpose of the MLCO training is to ensure that relevant employee(s) become aware of: • the Laws;

- the Company's Anti-Money Laundering Policy;
- the statutory obligations of the Company to report suspicious transactions;
- the employees own personal obligation to refrain from activity that would result in money laundering; and
- the importance of the Clients' due diligence and identification measures requirements for money laundering prevention purposes.

The MLCO shall be responsible to include information in respect of his/her education and training program(s) attended during the year in his/her Annual Report.

"=?];;;S;of;ocleousc

_____ Date; 09.03.2022

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 AMLCO

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

.....

.

.....

.

.....

.

.....

.

AMLCO DECISION

.....

.

.....

.

.....

. FILE NUMBER

.....

AMLCO 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 theClient.

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 financial instrument without obvious reason and in conditions that appear unusual (churning).

8. There are frequent small purchases of a particular financial instrument by a Client who settles in cash, and then the total number of the financial instrument 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 TerroristFinancing.

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 financial instruments 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 financial instruments, 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 the 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.

APPENDIX 4

PANAMA PAPERS INFORMATION				
Business relationship with persons (legal and natural), which are included into the Panama Papers or for which you have or had any business relationship with Mossack Fonseca				
A.	Name of legal/natural person			
B.	Nationality (applicable only to natural persons)			
C.	Country of incorporation (applicable only to legal persons)			
D.	Name of beneficial owners (applicable only to legal persons)			
E.	Nationality of beneficial owners			
F.	Business activities of legal/natural persons			
G.	Whether they are politically exposed persons			
H.	The investment services provided in accordance to Anti-Money Laundering Act,2006			
I.	ix. The AML/CFT risk categorisation (High/Normal/Low)			

J.	Reasoning if AML/CFT risk categorisation is HIGH (e.g. non-face-to-face, PEP, etc.)			
K.	Number of related internal suspicious reports and/or reports to the Unit			
L.	Reasoning if related internal suspicious reports and/or reports to the Unit were issued			
M.	Total inflows of money in the legal/natural person's client/bank accounts for the duration of the business relationship			
N.	Total outflows of money from the legal/natural person's client/bank accounts for the duration of the business relationship			
O.	Confirmation whether the total inflows/outflows of money is consistent with the information included in the client's economic profile (YES/NO)			