PREVENTION AND SUPPRESSION OF MONEY LAUNDERING & TERRORIST FINANCING

MANUAL

HOLBORN ASSETS WEALTH MANAGEMENT (CY) LTD

PREVENTION OF MONEY LAUNDERING & TERRORIST FINANCING MANUAL

1. GENERAL DEFINITIONS

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

ACES" is the Advisory Committee on Economic Sanctions formed by virtue of the Council of Ministers Decision dated 25 May 2012 under the presidency of the Minister of Finance, and reviews requests for the release of frozen assets under Sanctions and Restrictive Measures, and submits suggestions for their approval or rejection; final decision be taken by the Minister of Finance.

"**Advisory Authority/Unit**" means the Advisory Authority for Combating Money Laundering and Terrorist Financing which is established under Section 56 of the Law;

"**Beneficial Owner**" means the natural person or natural persons, who ultimately owns 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 corporate entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interests in that corporate entity, including through shareholdings, or through control via other means, other than accompany listed on a regulated market that is subject to the disclosure requirements consistent with European Union law, or subject to the equivalent international standards which ensure adequate transparency of ownership information:

Provided that:

a) an indication of direct shareholding shall be a shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a natural person; and

b) an indication of indirect ownership shall be a shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a corporate entity, which is under the control of a natural person, or by multiple corporate entities, which are under the control of the same natural person or persons.

Provided further that the control by other means can be verified, inter alia, based on the criteria provided for in section 142 (1) (b) and section 148 of the Companies Law;

ii. the natural person who holds the position of senior managing official if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under sub paragraph (i) of the present paragraph is identified, or if there is any doubt that the person identified is the beneficial owner.

Provided that the Company shall keep record of the actions taken in order to identify the beneficial ownership under sub paragraphs (i) and (ii);

(b) in the case of trusts:

i. the settlor;
ii. the trustee or commissioner;
iii. the protector, if any;
iv. the beneficiary, or where the individual benefiting from the legal arrangement or legal entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;
v. any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means; and

(c) in the case of legal entities, such as foundations, and legal arrangements similar to trusts, the natural person holding equivalent or similar positions to the persons referred to in paragraph (b);

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

"**Client**" means any legal or physical person aiming to conclude a Business Relationship or conduct an occasional transaction with the Company in or from the Republic. 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.

"Commission" means the Cyprus Securities and Exchange Commission.

"**Company**" means HOLBORN ASSETS WEALTH MANAGEMENT (CY) LTD which is incorporated in the Republic of Cyprus with registration number HE 401412.

"Directive" means the Prevention and Suppression of Money Laundering and Terrorist Financing Directive R.A.D. 157/2019, as amended, of the Cyprus Securities and Exchange Commission.

"**European Economic Area (EEA)**" means Member State of the European Union or other contracting state which is a party to the agreement for the European Economic Area signed in Porto on the 2nd of May 1992 and was adjusted by the Protocol signed in Brussels on the 17th of May 1993, as amended.

"**EU Directive**" means an act of the European Union entitled the Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the credit and financial system for the purpose of Money Laundering and Terrorist Financing, amendment of regulation (EU) number 648/2012 of the European Parliament and of the Council, and repealing directive 2005/60/EC of the European Parliament and of the Council and Directive 2006/70/EC of the Commission.

"High risk third country" means a third country, designated by the European Commission pursuant to the provisions of section 9 (2) of the EU Directive by the issuance of acts by way of derogation, which presents strategical shortcomings in its national system for combating money laundering and terrorist financing which are considered as important threats for the financial system of the European Union, and a third country, which is categorised by the Company as high risk in accordance with the risk assessment foreseen by section 58A of the Law.

"Illegal activities" means the predicate offences mentioned in section 5 of the Law.

"**Investment and Ancillary Services**" means the investment and ancillary services as per Part I and II of the First Appendix of the Law 87(I)/2017, for which the Company is licensed by the Cyprus Securities and Exchange Commission to offer.

"Joint Guidelines" are the Joint Risk Factor Guidelines under Articles 17 and 18(4) of EU Directive 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions, published by ESMA, EIOPA and EBA.

"**Manual**" means the Company's Prevention and Suppression of Money Laundering and Terrorist Financing Procedures Manual (this manual), according to the Directive.

"**Laundering Offences**" (or money laundering offences as known internationally) means the offences defined in Section 4 of the Law, as follows.

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 illegal activities, 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

commits an offence punishable by fourteen years' imprisonment or by a pecuniary penalty of up to Euro 500.000 or by both of these penalties in the case of (a) above and by five years' imprisonment or by a pecuniary penalty of up to Euro 50.000 or by both in the case of (b) above.

"**Law**" means the Prevention and Suppression of Money Laundering Activities Law of 2017, as amended.

"Obligated Entity" means any of the entities mentioned in section 2A of the Law.

"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:

(a) forming companies or other legal persons;
(b) 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;
(c) 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;
(d) acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement;
(e) acting as or arranging for another person to act as a nominee shareholder for another person.
(f) any of the services or activities specified in Article 4 of the Regulating Companies Providing Administrative Services and Related Matters Law, as amended or replaced.

"**Politically Exposed Person (PEP)**" means a natural person who is or has been entrusted with prominent public functions in the Republic or in another country , an immediate close relative of such person as well as a person known to be close associates of such a person:
Provided that, for the purpose of the present definition, 'prominent public function' means any of the following public functions:

(a) head of State, heads of government, ministers and deputy or assistant ministers;
(b) member of parliament or of similar legislative bodies;
(c) member of the governing bodies of political parties;
(d) member of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
(e) member of courts of auditors or of the boards of central banks;
(f) ambassador, chargés d'affaires and high-ranking officers in the armed forces;
(g) member of the administrative, management or supervisory bodies of State-owned enterprises;
(h) director, deputy director and member of the board or equivalent function of an international organisation;
(i) (mayor

Provided further that no public function referred to in points (a) to (i) shall be understood as covering middle-ranking or more junior officials (see also further details in Section 11.9.4 of the Manual);

Provided furthermore that 'close relatives of a politically exposed person' includes the following:
(a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;
(b) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;
(c) the parents of a politically exposed person;

Provided even furthermore that 'persons known to be close associates of a politically exposed person' means natural person:

(a) who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;
(b) who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

"**Predicate offence"** is any offence which is defined as a criminal offence by a law of the Republic.

(1) It is prohibited for a person trading in precious stones and/or precious metals, mechanical vehicles, works of art and/or antiques, within the framework of its business activities to receive any amount equal to or higher than ten thousand euros (€10.000) in cash, irrespective of whether the transaction is carried out in a single operation or in several operations which appear to be linked.

(2) A person trading in precious stones and/or precious metals, mechanical vehicles, works of art and/or antiques, in breach of the prohibition provided for in subsection (1), commits a criminal offence and, in case of conviction, is subject to a monetary fine not exceeding ten per-cent (10%) of the amount received in cash.

"**Republic**" means the Republic of Cyprus.

"**Regulated Market**" means a multilateral system which (a) is managed and/or operated by a market operator and (b) 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 authorised and functions regularly in accordance with the provisions of Part X of Law 87(I)/2018, or respective legislation of other member states that are enacted in compliance with Directive 2004/39/EC.

"**Sanctions Law"** is the Law on the Implementation of the Provisions of Security UN Council Resolutions or Decisions (Sanctions) and the Decisions and Regulation of the European Union (Restrictive Measures) Act 2016 (N. 58 (I)/ 2016)

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

"Terrorist Financing" means the provision or gathering of funds by any means, directly or indirectly, with the intention to use such funds or knowing that they will be used in whole or in part for the commission of an offence within the meaning given to the term by section 4 of the International Convention for the Suppression of the Financing of Terrorism (Ratification and Other Provisions) Law and by sections 5 to 13 of the Combating of Terrorism Law

"**Third Country**" means the country which is not a member of the European Union or contracting party to the European Economic Area Agreement, signed in Oporto on the 2nd of May 1992 and adjusted by the Protocol signed in Brussels on the 17th of May 1993, where the Agreement is thereafter, amended.

"Trust" means a written legal arrangement with which the settlor transfers property to one or more trustees who hold it for the benefit of one or more persons/beneficiaries.

'UIS' is the Unit for the Implementation of Sanctions in the Financial Sector in relation to Sanctions imposed by the UN Security Council Resolutions and Restrictive Measures imposed by the European Union (EU) Council Resolutions; the Unit was formed by virtue of the decision of the Ministerial Council dated 25 February 2016.

2. INTRODUCTION

The purpose of the Manual is to lay down the Company's internal practice, measures, procedures and controls relevant to the prevention and suppression 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 and suppression 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 Law, and the Directive of the Cyprus Securities and Exchange Commission (hereinafter "CySEC").

4. THE RESPONSIBILITIES OF THE BOARD OF DIRECTORS

4.1. General

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

(a) To have direct and continuous overview of the money laundering and terrorist financing issues;
(b) to determine, record and approve the general policy principles of the Company in relation to the prevention of Money Laundering and Terrorist Financing and communicate them to the AMLCO
(c) to appoint a senior official that possesses the skills, knowledge and expertise relevant to financial and other activities depending on the situation, who shall act as the 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 from CySEC
(d) to appoint, in case of the absence of the AMLCO, an Alternate AMLCO (hereinafter "Alternate AMLCO").
(e) to ensure that the Alternate AMLCO possesses the relevant skills, knowledge and expertise for carrying out the duties of the AMLCO as described in this Manual, the Law and the Directive.
(f) to approve the Manual and any updates thereof

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

(h) to ensure that the AMLCO, alternate AMLCO and his assistants, if any, and any other person who has been assigned with the duty of implementing the procedures for the prevention and suppression of Money Laundering and Terrorist Financing (i.e. personnel of the Administration/Back-Office Department), have complete and timely access to all data and information concerning Clients' identity, transactions' documents (as and where applicable) and other relevant files and information maintained by the Company so as to be fully facilitated in the effective execution of their duties, as included herein

(i) to ensure that all employees are aware of the person who has been assigned the duties of the AMLCO, as well as his assistants (if any), to whom they report, according to point (e) of Section 6.2 of the Manual any information concerning transactions and activities for which they have knowledge or suspicion that might be related to Money Laundering and Terrorist Financing

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

(k) to ensure that the AMLCO, and alternate AMLCO and their assistant AMLCOs, if any and the Administration/Back-Office Department have sufficient resources, including competent staff and technological equipment, for the effective discharge of their duties

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

(m) 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 in the manner described in Section 5 of the Manual. The minutes of the said decision of the Board and the Internal Auditor's report shall be submitted to CySEC 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).

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

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

(p) To approve the mandatory annual training program prepared by the AMLCO.

(q) To ensure that they receive adequate management information on the implementation of the Company's training program.

(r) To ensure to be adequately trained to be well aware and up-to-date with the Law, Directives and Circulars.

(s) To ensure that the training program of the Company includes the relevant Law, Directives and Circulars and further actions to mitigate any specific and unique vulnerability that the Company might have based on the Section 9 of the Manual.

The Company shall communicate immediately to the Commission, the names, the positions, as well as, the contact details of the persons it appoints as AMLCO, alternate AMLCO and where necessary assistant AMLCO.

4.2. BoD member responsible for AML

Pursuant to Article 58D of the Law, a member of the Board of Directors (in this section the BoD Member), is designated as the responsible person for the implementation of the legal framework related to the prevention and suppression of money laundering and terrorist financing.

Mr. Andreas Siapanis is the BoD member responsible for the implementation of the legal framework related to the prevention and suppression of money laundering and terrorist financing.

The BoD Member shall closely liaise with the Company's AMLCO for the purpose of devising guidelines and issuing broad instructions to the Company's various departments with a clear focus on ensuring continuous compliance with respect to AML. The AMLCO shall be then responsible to implement the guidelines and broad instructions issued by the BoD Member into efficient and transparent processes to be followed across the Company with respect to AML.

The Company shall ensure that the BoD Member receives the required resources and training for the dispensation of his duties.

5. OBLIGATIONS OF THE INTERNAL AUDITOR

5.1. General

The following obligations of the Internal Auditor are addressed specifically for the prevention and suppression 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 and suppression of Money Laundering and Terrorist Financing mentioned in the Manual
(b) the findings and observations of the Internal Auditor, in relation to point (a) above, shall be submitted, in a written report form, to the Board.

6. ANTI-MONEY LAUNDERING COMPLIANCE OFFICER

6.1. 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 duties adequately and efficiently.

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

In performing his 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.

6.2. Duties of the AMLCO

During the execution of his 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 9.5 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 internal practice, measures, procedures and controls relevant to the prevention and suppression 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 according to Section 10 of the Manual, 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 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 implement the guidelines and broad instructions issued by the member of the Board of Directors ('the BoD member') responsible for AML (pursuant to Article 58D of the Law and as per section 4.2 of the Manual), and create efficient and transparent processes to be followed across the Company, based on the said broad instructions and guidelines.

(f) 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

(g) 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

(h) if following the evaluation described in point (f) above, the AMLCO decides to notify the Money Laundering Combat Unit of the Republic (hereinafter the "Unit" or "MOKAS"), then he should complete an online report (Suspicious Transactions Reports/Suspicious Activities Reports ("STR/SAR")) on the web-application of the UNIT and submit it through the goAML Professional Edition (PE) system (https://reports.mokas.law.gov.cy/live/home) the soonest possible assuming that the Company has already registered with the relevant reporting system of the Unit. The Company shall ensure to maintain appropriate systems and procedures that allow the retrieval/reproduction of the said reports in hard copy at any given time. Subsequently to the submission of the STR/SAR to the Unit, the AMLCO shall be responsible for monitoring the procedure which shall follow and shall depend on the specificities of the case; the AMLCO shall take appropriate actions where requested by the Unit and as per the Unit's feedback policy.

The Unit will no longer provide interim or closing feedback on each STR/SAR submitted. The feedback policy of the Unit is as follows:

- Each electronically submitted STR/SAR will receive automatic acknowledgement of receipt, along with a corresponding reference number.
- As soon as an investigator is assigned to the STR/SAR by the Unit, the Company shall be informed accordingly.
- In exceptional cases and when deemed necessary by the Unit or if requested by the Company, feedback on specific cases, interim and /or final, will be provided.

- If administrative orders for postponement of transactions or for the monitoring of bank accounts are considered necessary, the Company will be informed accordingly.
- Periodically, the Unit will issues and distribute to the Company a report which will consist of sanitized cases, trends, indicators and statistics.
- The Annual Report of the Unit will be published and distrusted to the Company.
- Further to the above, the AMLCO shall be responsible to monitor this procedure and take appropriate actions.

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

(j) 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

(k) 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

(l) 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

(m) to identify the third person on whom the Company may rely for applying costumer due diligence identification procedures of the Clients, by providing his written consent for the relevant reliance. This written consent must be kept in personal records of the third person.

(n) 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.

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

(p) to acquire the knowledge and skills 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 15.2 of the Manual. Also, the AMLCO assesses the adequacy of the education and training provided

(r) to update the training programme of the Company accordingly, based on the relevant Law, Directives and Circulars.

(s) To ensure that the training program of the Company includes action for mitigating any specific and unique vulnerability that the Company might have, based on Section 9 of the Manual.
(t) to prepare correctly and submit timely to CySEC the monthly prevention statement of Section 8 of the Manual and provide the necessary explanation to the appropriate employees of the Company for its completion
(u) to prepare the Annual Report, according to Section 7 of the Manual
(v) to respond to all requests and queries from the Unit and CySEC, provide all requested information and fully cooperate with the Unit and CySEC
(w) 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 duties.
(x) to maintain a registry with the date/information of the third persons, that the Company relies and/or shall rely for applying the customer due diligence and identification procedures of the Clients.
(y) to ensure the preparation and maintenance of the list of Clients included in the Panama Papers (Appendix 4).

The above duties shall also duly be exercised by the alternate AMLCO in case of the absence of the AMLCO.

7. ANNUAL REPORT OF THE AMLCO

7.1. 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 to CySEC 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 and the Directive 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 and suppression 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, according to point (e) of Section 6.2 of the Manual and possible comments/observations thereon
(d) the number of reports submitted by the AMLCO to the Unit, according to point (g) of Section 6.2 of the Manual 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 Section 8 of the Manual. Any comments on material changes observed compared with the previous year are also reported
(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 agreements 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 Directive 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.

8. MONTHLY PREVENTION STATEMENT

8.1. General

The AMLCO shall prepare and submit to CySEC, according to point (q) of Section 6.2 of the Manual, on a monthly basis, the CySEC Form 144-08-11 "Monthly prevention statement regarding the prevention and suppression of Money Laundering and Terrorist Financing", which includes details as regards the total cash deposits accepted by the Company, the Internal Suspicions Reports, and the AMLCO's Reports to the Unit, according to points (e) and (g) in Section 6.2 of the Manual, respectively.

According to Circular CI144-2013-17, the aforementioned Form must be completed and submitted to CySEC within fifteen (15) days from the end of each month and the original completed and signed form must be kept in the Company's offices.

Following the issuance of the Circular C147, the scanned copy of the duly completed and signed Form 144-08-11 should be digitally signed and submitted to CySEC via the CySEC Web-Portal.

The completion of the aforementioned Form provides the opportunity to the Company initially to evaluate and, subsequently, to reinforce its systems of control and monitoring of its operations, for the purpose of early identification of transactions in cash which may be unusual and/or carry enhanced risk of being involved in Money Laundering and Terrorist Financing operations.

The Internal Auditor shall be responsible to review, at least annually as per Section 5.1 of the Manual, the submission to CySEC of the "Monthly prevention statement regarding the prevention and suppression of Money Laundering and Terrorist Financing".

9. RISK-BASED APPROACH

9.1. 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 Section of the Manual.

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

- recognises that the money laundering or terrorist financing threat varies across Clients, countries, services and financial instruments
- allows the Board to differentiate between Clients of the Company in a way that matches the risk of their particular business
- allows the Board to apply its own approach in the formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics
- helps to produce a more cost-effective system
- promotes the prioritisation of effort and actions of the Company in response to the likelihood of Money Laundering and Terrorist Financing occurring through the use of the Investment and Ancillary Services.

The risk-based approach adopted by the Company, and described in the Manual, involves specific measures and procedures in assessing the most cost effective and appropriate way to identify and manage the Money Laundering and Terrorist Financing risks faced by the Company. The Company should take into account the Joint Guidelines as well as the Guidelines issues by FATF.

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.

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 collection, movement and use of funds (with relation to terrorist financing)

The AMLCO shall be responsible for the development of the policies, procedures and controls on a risk-based approach. Further, the AMLCO shall also be responsible for the implementation of the policies, procedures and controls on a risk-based approach. The Internal Auditor shall be responsible for reviewing the adequate implementation of a risk-based approach by the AMLCO, at least annually, as per Section 5.1 of the Manual.

9.2. Identification of Risks

9.2.1. General/Principles

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 to CySEC 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.

9.2.2. Company Risks

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

(a) Risks based on the Client's nature:

- complexity of ownership structure of legal persons
- companies that have nominee shareholders or companies with bearer shares
- companies that are cash intensive
- companies incorporated in offshore centres
- PEPs
- Clients engaged in transactions which involves significant amounts of cash

- Client's or the beneficial owner businesses are commonly associated with higher corruption risk industry
- Client or the beneficial owner have links to sectors that are associated with higher money laundering and terrorist financing risk
- Client or the beneficial owner hold another prominent position or enjoy a high profile that enable the engagement to corruption
- Clients that are residents in countries of higher risk , i.e. countries as specified in Appendix 7 of the Manual:
- identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
- identified by credible sources as having significant levels of corruption or other criminal activity;
- subject to sanctions, embargos or similar measures issued by, for example, the European Union or United Nations;
- Providing funding or support terrorist activities, or that have designated terrorist organisations operating within their country.
- In case that the Client is a legal person, is engaged or established in countries of higher risk, as defined above.
- Clients included in the leaked documents of Mossack Fonseca (Panama Papers)
- Clients convicted for a Prescribed Offence (and already served their sentence) Client is a non-profit organization or charity fund (or other form of philanthropic organisation of charitable nature) whose activities could be abused for terrorist financing purposes.

(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.
- Client avoids the establishment of a business relationship, by carrying out one transaction or several one-off transactions.
- Age of client or beneficial owner does not match with the type of services/products sought.
- The sought products/services do not match with the Client's or beneficial owner's wealth situation.
- Client requests unnecessary or unreasonable levels of secrecy.

(c) Risks based on the Company's products, services and the nature/means of communication with the client:

- services that allow payments to/from unknown or un-associated third persons/parties
- large cash deposits or withdrawals
- products or transactions which may favour anonymity (pre-paid cards, virtual or crypto-currencies et al)

- new products and business practises, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.
- non face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures.
- Client has been introduced by a third party which is not part of the same group or its main business activity is unrelated to financial service provision.
- Client has been introduced by a tied agent, that is without direct contract with the Company
- high levels of cross border business which create exposure to Terrorist Financing risk

(d) *Risks associated with geographic and jurisdictional factors*

- The geographic position of the Company puts it at risk of being used as a transit station for people transporting assets for Terrorist Financing purposes.
- Bank deposits, investments, wire transfers, pre-paid cards of clients connected to focus jurisdictions (i.e. jurisdictions that present a higher risk of terrorism or which have strong geographical or other links with such countries) may pose a risk of Terrorist Financing for the Company.
- Persons associated with a client company (beneficial owners, relatives or associates of beneficial owners, persons exercising control over client company etc), which are from focus or high risk jurisdictions may pose a risk of Terrorist Financing for the Company.
- Assets held or activities undertaken by clients in focus jurisdictions or linked to such jurisdictions; business relationships or one-off transactions with parties who are in or are linked to focus jurisdictions.
- The jurisdictions of the PEPs are not relevant in determining the type of PEP, but the domicile or nationality of the PEP is relevant to the risk. Foreign PEPs always impose higher risk than domestic PEPs.

9.2.3. Sources of Information

The Company shall collect information, for assessing the Money Laundering and Terrorist Financing, from a variety of sources, whether these are accessed individually or through commercial databases that pool information from several sources.

1. The Company shall always consider the following source of information:

the European Commission's supranational risk assessment; the European Commission's list of high-risk third countries;

- information from government, such as the National Assessment of Money Laundering and Terrorist Financing Risks, policy statements and alerts, and explanatory memorandums to relevant legislation;
- information from the competent authorities, such as guidance and the reasoning set out in regulatory fines;
- information from Financial Intelligence Units (FIUs) and law enforcement agencies, such as threat reports, alerts and typologies; and

- information obtained as part of the initial CDD process.

2. Other sources of information firms may consider in this context may include, among others:
   - the Company's own knowledge and professional expertise;
   - information from industry bodies, such as typologies and emerging risks;
   - information from civil society, such as corruption indices and country reports;
   - information from international standard-setting bodies such as mutual evaluation reports or legally non-binding blacklists;
   - information from credible and reliable open sources, such as reports in reputable newspapers;
   - information from credible and reliable commercial organisations, such as risk and intelligence reports; and
   - information from statistical organisations and academia.

The referred sources shall be used also for the implementation of Sections 10, 11 and 12 of the respective Manual.

9.3. 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
- requiring the quality and extent of required identification data for each type of Client to be of a certain standard (e.g. documents from independent and reliable sources, third person information, documentary evidence)
- obtaining additional data and information from the Clients, where this is appropriate for the proper and complete understanding of their activities and source of wealth and for the effective management of any increased risk emanating from the particular Business Relationship or the Occasional Transaction
- on-going monitoring of high-risk Clients' transactions and activities, as and when applicable
- obtaining tools and software which shall permit the proper identification of transactions, individuals, entities or jurisdictions which are subject to international sanctions.
- good understanding of Fintech, Regtech, block chain and other developing technologies and the way these might be offered or used for money laundering or terrorist financing purposes.

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 Sections 10 and 11 of the 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.

9.4. 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.

9.5. 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 Administration/Back-Office Department shall consult data, information and reports [e.g. Clients from countries which inadequately apply Financial Action Task Force's (hereinafter "FATF"), country assessment reports] that are published in the following relevant international organisations

(a) FATF - www.fatf-gafi.org
(b) The 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) the Joint Committee European Supervisory Authorities - https://esasjoint-committee.europa.eu/
(h) The Ministry of Foreign Affairs in relation to international sanctions by the UN Security Council, and restrictive measures of the Council of the EU - http://www.mfa.gov.cy/mfa/mfa2016.nsf/mfa35_en/mfa35_en?OpenDocument
(i) the EU Sanctions Map - https://www.sanctionsmap.eu/#/main

10. CLIENT ACCEPTANCE POLICY

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

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

The Internal Auditor shall review and evaluate the adequate implementation of the CAP and its relevant provisions, at least annually, as per Section 5 of the Manual.

10.1. General Principles of the CAP

The General Principles of the CAP are the following:

(a) the Company shall classify Clients into various risk categories and based on the risk perception decide on the acceptance criteria for each category of Client
(b) where the Client is a prospective Client, an account must be opened only after the relevant pre-account opening due diligence and identification measures and procedures have been conducted, according to the principles and procedures set in Section 11 of the Manual
(c) all documents and data described in Section 11.6 of the Manual must be collected before the establishment of a business relationship with a new Client
(d) by way of derogation of point (c) above and according to Section 11.5(2) of the Manual, the verification of the identity of a new Client may be completed during the establishment of the business relationship
(e) no account shall be opened in anonymous or fictitious names(s)
(f) no account shall be opened unless the prospective Client is approved by the:
    - The Head of the Administration/Back Office Department

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

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

10.2.1. Low Risk Clients

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

Moreover, the Company shall follow the *Simplified Client Identification and Due Diligence Procedures* for low risk Clients, according to Section 11.8 of the Manual.

10.2.2. Normal Risk Clients

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

10.2.3. High Risk Clients

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

Moreover, the Company shall apply the *Enhanced Client Identification and Due Diligence* measures for high risk Clients, according to Section 11.9 of the Manual and the due diligence and identification procedures for the specific types of high risk Clients mentioned as well in Section 11.10 of the Manual, as applicable.

10.3. 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 his identity and the creation of his economic profile, without adequate justification.
- Shell Banks.
- Clients included in Sanctions Lists.
- Clients convicted for a Prescribed Offence (and not served their sentence)
- Credit institutions, financial organisations and legal persons that operate in the areas of the Republic of Cyprus under Turkish military occupation, which are not incorporated according to the laws of the Republic of Cyprus and do not possess operating licence for providing services from CySEC or any other relevant regulatory authority of the Republic of Cyprus, in view of Circular CI144-2008-11.
- Clients that settle their transactions with the Company with cash.
- Clients from OFAC countries.

10.4. Client Categorisation Criteria

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

10.4.1. Low Risk Clients

The Company may apply simplified due diligence procedures in case where the professional relationship with the client or the transaction is of low risk. Appendix 5 of the Manual refers to a list of factors and types of evidence of potentially lower risk of money laundering and terrorist financing that need to be examined, in order for the

AMLCO to decide if the Client will be categorized as low-risk. The Company shall gather adequate information in order to be able to conclude that the professional relationship or transaction is indeed of low risk. In the course of the said assessment for the determination of the above, the Company shall pay particular attention to every activity of these clients or each transaction which may, given its nature, be considered as particularly likely to be linked to money laundering or terrorist financing.

In this respect, the AMLCO shall be responsible to gather the said information. The said information shall be duly documented and filed, as applicable, according to the recording keeping procedures described in Section 14.

10.4.2. Normal Risk Clients

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

- any Client who does not fall under the 'low risk Clients' or 'high risk Clients' categories set in Sections 10.4.1 and 10.4.3, respectively.

10.4.3. High Risk Clients

The Company shall consider Appendix 6 of the Manual referring to the list of factors and types of evidence of potentially higher risk of money laundering and terrorist financing, that need to be examined, in order for the AMLCO to decide if the Client will be categorized as high-risk.

In the following types/cases of Clients there is potentially higher risk of Money Laundering and Terrorist Financing and hence clients may be considered as high risk in terms of Money Laundering and Terrorist Financing:

- Clients that are residents in high risk third-countries, i.e. countries (as specified in of Appendix 7 of the Manual):
    - identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
    - identified by credible sources as having significant levels of corruption or other criminal activity;
    - subject to sanctions, embargos or similar measures issued by, for example, the European Union or United Nations;
    - providing funding or support terrorist activities, or that have designated terrorist organisations operating within their country.
- Clients whose own shares or those of their parent companies (if any) have been issued in bearer form
- Non-face-to-face business with clients, without certain safeguards, such as electronic signatures.

- Trust accounts
- Transactions or business relationships with a PEP
- Clients from countries which inadequately apply FATF's recommendations
- Cross border correspondent relationships with a third-country respondent institution, a credit institution and financial institution
- Clients included in the leaked documents of Mossack Fonseca (Panama Papers)

The Company, if possible, shall conduct face-to-face meeting with the high-risk clients before accepting them or continuing the business relationship.

11. CLIENT DUE DILIGENCE AND IDENTIFICATION PROCEDURES

11.1. 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 15,000 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 of the amount of the transaction or any derogation, exemption or minimum threshold pursuant to the provisions of the Law;
(d) when there are doubts about the veracity or adequacy of previously held Client identification data.

In this respect, it is the duty of the AMLCO to apply all the relevant Client Due Diligence Identification Procedures described in Section 11 of the Manual for the four (4) cases mentioned above. Furthermore, the Administration/Back-Office Department shall also be responsible to collect and file the relevant Client identification documents, according to the recording keeping procedures described in Section 14 of the Manual.

Further, the AMLCO shall be responsible to maintain at all times and use during the application of Client due diligence and identification procedures template-checklists with respect to required documents and data from potential Clients, as per the requirements of the Law and the Directive.

If Remote Customer Onboarding (identification process) is performed, please refer to APPENDIX 8 GUIDELINES of this manual.

The Internal Auditor shall be responsible to review the adequate implementation of all the policies and procedures mentioned in Section 5.1 of the Manual, at least annually.

11.2. 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 independent source. It is noted that the identification procedure includes the following:
    i. Creation of an economic profile for the customer/beneficial owner,
(b) Carrying out an appropriateness test in accordance to article 26(3)(a) of the L.87(I)/2017. 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) assessing and depending on the case, obtaining information on the purpose and intended nature of the business relationship
(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.
(e) Screening Clients against automated databases or third party checks for adverse tax-related news. Screening shall be performed prior the:
    i. The establishment of business relationship;
    ii. The provision of the any services; and
    iii. Undertaking any transaction for a customer.

(f) Checking Clients against databases with regards to European Union, United Nations and International Sanctions

The Company applies each of the customer due diligence measures and identification procedures set out above, but may determine the extent of such measures on a risk sensitive basis depending on the purpose of the account or business relationship, the level of assets to be deposited by the client, or the size of transactions undertaken, and the regularity or duration of the business relationship.

Any data and information collected from the clients shall be assessed based on the Section 9 of the Manual.

11.3. 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 signature or that he is the real owner of the account or that he 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.

11.4. 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 identity and the creation of his economic profile (see Section 11.6 of the Manual), 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 (see Section 10.3 of the Manual) while at the same time the AMLCO considers whether it is justified under the circumstances to submit a report to the Unit, according to point (g) of Section 6.2 of the Manual.

If, during the Business Relationship, a Client fails or refuses to submit, within a reasonable timeframe, the required verification data and information according to Section 11 of the Manual, the Company and the AMLCO shall consider terminating the Business Relationship and terminate the agreement with 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, according to paragraph point (g) of Section 6.2 of the Manual.

11.5. Time of Application of the Client Identification and Due Diligence Procedures

With respect to the timing of the application of the Client Identification and Due Diligence Procedures, the AMLCO shall be responsible for the application of the following provisions:

1. The verification of the identity of the Client and the Beneficial Owner shall be performed before the establishment of a Business Relationship or the carrying out of a transaction.

2. By way of derogation from point (1) above, the verification of the identity of the customer and the beneficial owner shall 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 **and** the process of verification is completed as soon as practicable after the initial contact.

   For the purposes of this point, the risk of money laundering or terrorist financing may be assessed as low when, as a minimum, the following, among others, are taken into consideration:

- The cumulative time in which the verification of the identity of a customer/beneficial owner is completed, must not exceed 15 days from initial contact.
- It is noted that the initial contact takes place the moment that the client either accepts the terms and conditions or makes his first deposit, whichever comes first.
- Within the timeframe of 15 days from initial contact, the regulated entity takes all reasonable measures to ensure that the percentage of customers that have not complied with the request to submit verification documents, is considerably low (e.g. the Company issues requests/reminders to the customer/beneficial owner informing them of their obligation to submit the requested documents for the verification of their identity).
- Where the verification of the customer/beneficial owner's identity has not been completed during the designated timeframe of 15 days, the commencement of a business relationship must be terminated on the date of the deadline's expiry and all deposited funds must be returned to the customer/beneficial owner, in the same bank account from which they originated in case where the Company offers services relating to safekeeping of clients funds and assets. The procedure for returning the funds must occur immediately, regardless of whether the customer has requested the return of their funds or not. The returned funds (deposits) include any profits the customer has gained during their transactions and deducting any losses incurred.
- Within the timeframe of 15 days from initial contact, the customer/beneficial owner must undergo at least one Enhanced Due Diligence measure in accordance to article 64 of the Law.
- No funds are withheld and no accounts are frozen, save for those cases of suspicion of money laundering, where the regulated entity is under obligation to immediately report their suspicion to MOKAS and notify CySEC (through the Monthly Prevention Statement) of the suspicious transaction incident in the designated procedure (please refer to Section 8 of this Manual).

It is noted that the Company shall complete the prescribed procedures for the verification of customers' identity before the establishment of a business relationship. In those cases where the verification of a customer or beneficial owner's identity takes place during the establishment of a business relationship (after the initial contact), the Company shall take into consideration this point of the Manual as well as the designated internal procedure that is attached hereto as Appendix 6.

3. In cases where the Company is unable to comply with points (a) to (j) of Section 11.2 of the Manual, the Company shall not , establish a Business Relationship or carry out the transaction, or depending on the case, shall terminate the business relationship and shall consider making a report to the Unit.

Identification procedures and Client due diligence requirements shall be applied not only to all new Clients but also to existing Clients at appropriate times (see points (b) to (d) of Section 11.1 of the Manual), depending on the level of risk of being involved in money laundering or terrorist financing among others, at times when the relevant circumstances of the client change.

11.6. 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/follow the principles below:

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

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

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

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

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

- the purpose and the reason for requesting the establishment of a Business Relationship
- the anticipated account turnover, the nature of the transactionsthe Client's size of wealth and annual income and the clear description of the main business/professional activities/operations

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

- the name of the company
- the country of its incorporation
- the head offices address and registered 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
- Memorandum and Articles of Association of the company
- the ownership structure of the group that the Client-legal person may be a part of (country of incorporation of the parent company, subsidiary companies and associate companies, main activities and financial information).

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

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

(h) Client transactions transmitted for execution, shall be compared and evaluated against the anticipated account's turnover, the usual turnover of the activities/operations of the Client and the data and information kept for the Client's economic profile. Significant deviations are investigated, and the findings are recorded in the respective Client's file. Transactions that are not justified by the available information on the Client are thoroughly examined so as to determine whether suspicions over money laundering or terrorist financing arise for the purposes of submitting an internal report to the AMLCO, according Section 6.2 of the Manual.

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. The Company shall be able to demonstrate to CySEC that the extent of the measures is appropriate in view of the risks of the use of the Investment and Ancillary Services for the purposes of Money Laundering and Terrorist Financing.

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

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

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

The construction of the Client's economic profile according to the provisions above shall be undertaken by the AMLCO. In this respect, the data and information collected for the

construction of the economic profile shall be fully documented and filed, as applicable, by the Administration/Back-Office Department.

11.7. <u>Further Obligations for Client Identification and Due Diligence Procedures</u>

1. In addition to the principles described in Section 11.6. above, the Company, and specifically the AMLCO shall:

   (a) ensure that the Client identification records remain completely updated with all relevant identification data and information throughout the Business Relationship
   (b) examine and check, on a regular basis, the validity and adequacy of the Client identification data and information that he maintains, especially those concerning high risk Clients.

   The procedures and controls of point (a) in Section 6.2 of the Manual also determine implicitly the timeframe during which the regular review, examination and update of the Client identification is conducted. The outcome of the said review shall be recorded in a separate note/form which shall be kept in the respective Client file.

2. Despite the obligation described in point (1) above and while taking into consideration the level of risk, if at any time during the Business Relationship, the Company becomes aware that reliable or adequate data and information are missing from the identity and the economic profile of the Client, then the Company takes all necessary action, by applying the Client identification and due diligence procedures according to the Manual, to collect the missing data and information, the soonest possible, so as to identify the Client and update and complete the Client's economic profile.

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:

   (a) an important transaction takes place which appears to be unusual and/or significant compared to the normal pattern of transactions and the economic profile of the Client
   (b) a material change in the Client's legal status and situation, such as:
      i. change of directors/secretary
      ii. change of registered shareholders and/or Beneficial Owners
      iii. change of registered office
      iv. change of trustees
      v. change of corporate name and/or trading name
      vi. change of the principal trading partners and/or undertaking of major new business activities
   (c) a material change in the way and the rules the Client's agreement operates, such as:
      i. change in the persons that are authorised to operate the agreement

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

(a) .

11.8. Simplified Client Identification and Due Diligence Procedures

The Company may apply simplified Client Identification and Due Diligence Procedures, provided that it will ensure that the business relationship or the transaction is low risk.

In this respect, the Company ensures to carry out sufficient information in order to be able to conclude that the professional relationship is indeed of low risk and enable the detection of unusual or suspicious transactions.

When assessing the risks of money laundering, the Company takes into account at least the factors of potentially lower risk situations, as specified in Appendix 5 of the Manual.

In particular, 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. Nevertheless, the Company will carry out background checks on the client to ensure that the risk of money laundering and terrorist financing is indeed lower;

2. In addition to the above, the Company must exercise continuous monitoring of the business relationships mentioned in Section 10.4.1 according to the provisions of the paragraph (d) of Section 11.2. or report to the Unit any suspicious transaction or any attempt to carry out a suspicious transaction

3. Further to the above, CySEC may permit simplified KYC for low risk products and transactions, subject to specific criteria as defined in the AML Law as amended.

4. It is provided that the Company shall collect sufficient information, so as to decide whether the Client can be exempted according to the provisions of point (1) - already mentioned in Section 10.4.1. The Company when assessing the abovementioned 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.

5. 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.

6. With respect to public authorities or public bodies of the EEA countries, for which the provisions of point (1) of Section 11.6 may not 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.

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

11.9.1. General Provisions

The AMLCO shall apply enhanced due diligence measures, in addition to the measures referred to in Sections 11.2, 11.5, 11.6 and 11.7, in the following cases:

(a) When the Company is transacting or establishes a business relationship with a natural person that is resident in a high-risk third country and/or with a legal entity established in a high risk third-country.

In such a case, enhanced customer due diligence measures will not be automatically applied with respect to branches or majority owned subsidiaries of the Company established in the European Union which are located in high-risk third countries, where those branches or majority owned subsidiaries fully comply with the group-wide policies and procedures in accordance with the provisions of section 68A of the Law and, in such a case, the Company uses the risk-based approach;

(b) In respect of cross-frontier correspondent banking relationships with credit institutions-Clients from third countries, the Company shall:

i. gather sufficient information about the credit institution-Client to understand fully the nature of the business and the activities of the Client and to assess, from publicly available information, the reputation of the institution and the quality of its supervision
ii. assess the systems and procedures applied by the credit institution-Client for the prevention and suppression of Money Laundering and Terrorist Financing

iii. obtain approval from the *Senior Management* before entering into correspondent bank account relationship

iv. document the respective responsibilities of the person engaged in financial or Other Business Activities and of the credit institution-Client

v. with respect to payable-through accounts, must be ensured that the credit institution-Client has verified the identity of its Clients and performed on-going due diligence on the Clients having direct access to the correspondent bank accounts and that it is able to provide relevant Client's due diligence data to the correspondent institution, upon request.

(c) With respect to transactions or Business Relationships with PEPs, the Company shall:

i. establish appropriate risk management procedures for verifying whether the client is a politically exposed person. Such procedures may include, depending on the level of risk, the instalment of the reliable electronic data base for politically exposed persons, the research and collection of information from the client or publically available information. In case of legal entities and arrangements, the procedures aim to the verification of the political exposure of the ultimate beneficial owners, authorized signatories and persons duly authorized to act on half of the aforementioned. In such a case where one of the above is a politically exposed person, the account of the legal entity or arrangement is subject to the relevant procedures to be followed for a politically exposed natural person.

ii. 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. The AMLCO must have been informed in relation to both of the above scenarios.

iii. take adequate measures to establish the economic profile of the client including his source of wealth and source of funds. Evidence must be regularly collected and renewed with respect to the nature and size of the client's transactions which are subject to regular monitoring. The Company shall be particularly attentive and diligent when the client's activities are associated with corruption such as the trading of oil, cigarettes and alcoholic beverages;

iv. conduct enhanced on-going monitoring of the Business Relationship and reviewed on an annual basis with respect to its continuation. The relationship manager of the account shall prepare a short report with the results of the review. The report shall be submitted to the Board for studying and approval and is filed in the client';

v. apply the measures referred to in points (i), (ii), (iii) and (iv) to family members or to the persons which are known to be close associates of a PEP.

For further details see Section 11.9.2 below.

d) With respect to non-face-to-face business relationships or transactions, where there is no physical presence of the parties, without certain safeguards, such as electronic signatures, there is high risk of money laundering or terrorism financing: the Company shall apply the following at minimum:

i. Make the first payment, in the context of the transaction or the Business Relationship, via a bank account which has been opened in the Client's name, and is maintained to a credit institution which is operated and is licensed is an European Economic Area country or in a low-risk country, as listed in the Appendix 5, para 3 of this Manual;

ii. The Company shall immediately be provided with confirmation from a credit institution, engaged in a business relationship with the Client. The respective confirmation must indicate the name, the address and the passport number of the Client.

e) With respect to accounts in names of companies whose shares are in bearer form, the AMLCO shall apply the following:

I. The Company may accept a request for the establishment of a Business Relationship or for an Occasional Transaction from companies whose own shares or those of their parent companies (if any) have been issued in bearer form by applying, in addition to the procedures of Section 11.10.6, all the following supplementary due diligence measures:

(a) the Company takes physical custody of the bearer share certificates while the Business Relationship is maintained or obtains a confirmation from a bank operating in the Republic or a country of the EEA that it has under its own custody the bearer share certificates and, in case of transferring their ownership to another person, shall inform the Company accordingly

(b) the business relationship is closely monitored throughout its operation. At least once a year, a review of the accounts' transactions and turnover is carried out and a note is prepared summarising the results of the review which shall be kept in the Client's file

(c) if the entering into a business relationship has been recommended by a third person as defined in Section 11.11, at least once every year, the third person who has introduced the Client provides a written confirmation that the capital base and the shareholding structure of the company-Client or that of its holding company (if any) has not been altered by the issue of new bearer shares or the cancellation of existing ones. If the business relationship has been entered into directly by the company-Client, then the written confirmation is provided by the company-Client's directors

(d) when there is a change to the Beneficial Owners, the Company examines whether or not to permit the continuance of the relationship.

f) With respect to Clients from countries which inadequately apply FATF's recommendations

i. 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.

ii. transactions with persons from the said countries, for which there is no apparent economic or visible lawful purpose, are further examined for the establishment of their economic or business background and purpose. If the Company cannot be fully satisfied as to the legitimacy of a transaction, then a suspicious transaction report is filed to the Unit, according to point Section 6.2 of the Manual.

11.9.2. Account in names of companies whose shares are in bearer form

The AMLCO shall apply the following with respect to agreements in names of companies whose shares are in bearer form:

1. The Company may accept a request for the establishment of a Business Relationship or for an Occasional Transaction from companies whose own shares or those of their parent companies (if any) have been issued in bearer form by applying, in addition to the procedures of Section 11.10.6, all the following supplementary due diligence measures:

   (a) the Company takes physical custody of the bearer share certificates while the Business Relationship is maintained or obtains a confirmation from a bank operating in the Republic or a country of the EEA that it has under its own custody the bearer share certificates and, in case of transferring their ownership to another person, shall inform the Company accordingly
   (b) the account is closely monitored throughout its operation. At least once a year, a review of the accounts' transactions and turnover is carried out and a note is prepared summarising the results of the review which shall be kept in the Client's file
   (c) if the opening of the account has been recommended by a third person as defined in Section 11.11, at least once every year, the third person who has introduced the Client provides a written confirmation that the capital base and the shareholding structure of the company-Client or that of its holding company (if any) has not been altered by the issue of new bearer shares or the cancellation of existing ones. If the account has been opened directly by the company-Client, then the written confirmation is provided by the company-Client's directors

(d) when here is a change to the Beneficial Owners, the Company examines whether or not to permit the continuance of the account's operation.

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

With respect to Clients from countries which inadequately apply FATF's recommendations, the Company shall:

i. 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.

ii. transactions with persons from the said countries, for which there is no apparent economic or visible lawful purpose, are further examined for the establishment of their economic or business background and purpose. If the Company cannot be fully satisfied as to the legitimacy of a transaction, then a suspicious transaction report is filed to the Unit, according to point (g) Section 6.2 of the Manual.

11.9.4. "Politically Exposed Persons" agreements

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

1. The establishment of a Business Relationship or the execution of an Occasional Transaction with politically exposed persons as interpreted in Article 2(1) of the Law, may expose the Company to enhanced risks, especially if the potential Client seeking to establish a Business Relationship or the execution of an Occasional Transaction is a PEP, a member of his immediate family or a close associate that is known to be associated with a PEP.

   The Company shall pay more attention when the said persons 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.

2. In order to effectively manage such risks, the Company shall assess the countries of origin of its Clients in order to identify the ones that are more vulnerable to corruption or maintain laws and regulations that do not meet the 40 requirements of the FATF.

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

With regard to the issue of adequacy of application of the 40 recommendations of the FATF, the Company shall retrieve information from the country assessment reports prepared by the FATF or other regional bodies operating in accordance with FATF's principles (e.g. Moneyval Committee of the Council of Europe) or the International Monetary Fund.

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

   (a) heads of State, heads of government, ministers and deputy or assistant ministers
   (b) members of parliament or of similar legislative bodies
   (c) members of the governing bodies of political parties
   (d) 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
   (e) members of courts of auditors or of the boards of central banks
   (f) ambassadors, chargıs d'affaires and high-ranking officers in the armed forces
   (g) members of the administrative, management or supervisory bodies of State-owned enterprises.
   (h) Directors, deputy directors and members of the board of equivalent function of an international organisation;
   (i) Mayors.

4. Where a politically exposed person is no longer entrusted with a prominent public function by the Republic or a member state or a third country, or with a prominent public function by an international organisation, the Company shall, for at least 12 months, be required to take into account the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to politically exposed persons.

5. None of the categories set out in point (4) above shall be understood as covering middle ranking or more junior officials. Close relatives of PEPs 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 of the PEP.

6. '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 PEP

(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 facto of the PEP.

7. Without prejudice to the provisions of point (c) Section 11.9.1 of the Manual, the Company adopts the following additional due diligence measures when it establishes a Business Relationship or carry out an Occasional Transaction with a PEP:

(a) the Company puts in place appropriate risk management procedures to enable it to determine whether a prospective Client is a PEP. Such procedures may include, depending on the degree of risk, the acquisition and installation of a reliable commercial electronic database for PEPs, seeking and obtaining information from the Client himself or from publicly available information. In the case of legal entities and arrangements, the procedures will aim at verifying whether the Beneficial Owners, authorised signatories and persons authorised to act on behalf of the legal entities and arrangements constitute PEPs. In case of identifying one of the above as a PEP, then automatically the account of the legal entity or arrangement should be subject to the relevant procedures specified in this Section of the Manual

(b) the decision for establishing a Business Relationship or the execution of an Occasional Transaction with a PEP is taken by the Senior Management of the Company and the decision is then forwarded to the AMLCO. When establishing a Business Relationship with a Client (natural or legal person) and subsequently it is ascertained that the persons involved are or have become PEPs, then an approval is given for continuing the operation of the Business Relationship by the Senior Management of the Company which is then forwarded to the AMLCO

(c) before establishing a Business Relationship with 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)

(d) the Company shall create the economic profile of the Client by obtaining the information specified in Section 11.6. The details of the expected business and nature of activities of the Client forms the basis for the future monitoring of the relationship. 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

(e) the agreement shall be subject to annual review in order to determine whether to allow its continuance of operation. A short report shall be prepared summarising the results of the review by the person who is in charge of monitoring the relationship. The report shall be submitted for consideration and approval to the Board and filed in the Client's personal file.

11.9.5. Electronic gambling/gaming through the internet

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

1. 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 or a third country which, in accordance with a relevant decision of the Advisory Authority it has been determined that the relevant third country applies procedures equivalent to the requirements of the EU Directive. For this purpose, the Company shall request and obtain, apart from the data and information required by the Manual, copy of the licence 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.

2. 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 and suppression of money laundering and terrorist financing.

3. 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 point (1) above, then the Company shall request and obtain, apart from the data and information required by the Manual, 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 point (1) 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 an *Executive Director* of the Company and the decision is then forwarded to the AMLCO. 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.

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

1. Further to the issuance of CySEC Circulars C125 and C132, in relation to the leaked documents of Mossack Fonseca which refers to persons who may be involved in tax evasion, corruption and/or money laundering activities (colloquially known as the "**Panama Papers**") the Company shall categorise such clients as High Risk with respect to the Money Laundering and Terrorist Financing risk which the Company faces.

   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 Papers[1] 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 Mossack Fonseca;

   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 Section of the 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 Section 11.5.2 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.

3. With respect to transactions or Business Relationships with clients subject to this Section of the Manual, the AMLCO shall:

   a. apply enhanced due diligence measures for identifying and monitoring such clients, as prescribed in this Manual;
   b. collect adequate information so as to understand the clients' profile;
   c. take supplementary measures to verify or certify the documents supplied, or require confirmatory certification by a credit or financial institution covered by the EU Directive or
   d. ensure that the first payment of the operations is carried out through an account opened in the client's name with a credit institution which operates in a country within the EEA;
   e. take adequate measures to establish the source of wealth and source of funds that are involved in the Business Relationship or transaction by collecting relevant evidence;

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

f. conduct enhanced on-going monitoring of the Business Relationship;
g. 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);
h. seek and obtain information from the client himself or from publicly available information (incl. the reliable commercial electronic database used by the Company);
i. create the economic profile of the client by obtaining the information specified in this Manual. The details of the expected business and nature of activities of the client forms the basis for the future monitoring of the relationship. The profile shall be regularly reviewed and updated with new data and information;
j. review on an annual basis the clients' agreement in order to determine whether to allow its continuance of operation. A short report shall be prepared summarising the results of the review by the AMLCO. The report shall be submitted for consideration and approval to the Board and filed in the client's personal file;

4. Transactions with persons subject to this Section of the Manual, for which there is no apparent economic or visible lawful purpose, are further examined for the establishment of their economic, business or investment background and purpose. If the Company cannot be fully satisfied as to the legitimacy of a transaction, then a suspicious transaction report is filed to the MOKAS.

5. The AMLCO should keep records of Clients subject to this Section of the Manual as prescribed in Appendix 5 below.

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

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

11.10.1. Natural persons residing in the Republic of Cyprus

1. The Company shall obtain the following information to ascertain the true identity of the natural persons residing in the Republic:
   (a) true name and/or names used as these are stated on the official identity card or passport
   (b) full permanent address in the Republic, including postal code
   (c) telephone (home and mobile) and fax numbers
   (d) e-mail address, if any
   (e) date and place of birth
   (f) nationality and
   (g) details of the profession and other occupations of the Client including the name of employer/business organisation.

2. 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 Licence 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 AMLCO 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.

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

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

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

5. 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.

11.10.2. Natural persons not residing in the Republic

1. The Company shall obtain the information described in Section 11.10.1 to ascertain the true identity of the natural persons not residing in the Republic.

2. 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.

3. 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.

11.10.3. Joint accounts

In the cases of joint agreements of two or more persons, the identity of all individuals that hold or have the right to manage the account, are verified according to the procedures set in Sections 11.10.1 and 11.10.2 above.

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

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

Furthermore, the Company shall obtain a list of the members of board of directors/management committee of the abovementioned organisations and verifies the identity of all individuals that have been authorised to manage the account according to the procedures set in Sections 11.10.1 and 11.10.2.

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

1. In the case of unincorporated businesses, partnerships and other persons with no legal substance, the identity of the directors, partners, Beneficial Owners and other individuals who are authorised to manage the account shall be verified according to the procedures set in Sections 11.10.1 and 11.10.2.

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

2. The Company shall obtain documentary evidence of the head office address of the business, ascertains the nature and size of its activities and receives all the information

required according to Section 11.6 for the creation of the economic profile of the business.

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

11.10.6. Accounts of legal persons

1. 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 set in Sections 11.10.1 and 11.10.2.

2. 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 set in Sections 11.10.1 and 11.10.2.

3. 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:

   (a) the registered number
   (b) the registered corporate name and trading name used
   (c) the full addresses of the registered office and the head offices
   (d) the telephone numbers, fax numbers and e-mail address
   (e) the members of the board of directors
   (f) the individuals that are duly authorised to operate the account and to act on behalf of the legal person
   (g) the Beneficial Owners of private companies and public companies that are not listed in a Regulated Market of an EEA country or a third country with equivalent disclosure and transparency requirements
   (h) the registered shareholders that act as nominees of the Beneficial Owners
   (i) the economic profile of the legal person, according to the provisions of Section 11.6.

4. 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:

   (a) certificate of incorporation and certificate of good standing (where available) of the legal person
   (b) certificate of registered office

(c) certificate of directors and secretary
(d) 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 or a third country with equivalent disclosure and transparency requirements
(e) memorandum and articles of association of the legal person
(f) 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
(g) 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
(h) documents and data for the verification, according to the procedures set in Sections 11.10.1 and 11.10.2, 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.

5. 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.

6. For legal persons incorporated outside the Republic, the Company requests and obtains documents similar to the above.
7. 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.

8. 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, registered in the Republic or abroad, 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.

9. 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 10% in the legal person's ordinary share capital or voting rights.

10. In cases where the Beneficial Owner of a legal person, requesting the establishment of a Business Relationship or the execution of an Occasional Transaction, is a trust set up in the Republic or abroad, the Company shall implement the following procedure:

    (a) 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, according to the procedures set in Sections 11.10.1 and 11.10.2
    (b) 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.

11.10.7. Investment funds, mutual funds and firms providing financial or investment services

1. The Company shall establish and maintain Business Relationships or execute Occasional Transactions with persons who carry out the above services and activities which are incorporated and/or operating in countries of the EEA or a third country which according to a relevant decision of the Advisory Authority it has been determined that applies requirements equivalent to those laid down in the EU Directive,) provided that the said persons:

    (a) possess the necessary licence or authorisation from a competent supervisory/regulatory authority of the country of their incorporation and operation to provide the said services, and

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

2. 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 other than those mentioned in point (1) above, the 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 licence 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.

3. 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.

11.10.8. Nominees or agents of third persons

1. The Company shall take reasonable measures to obtain adequate documents, data or information for the purpose of establishing and verifying the identity, according to the procedures set in Sections 11.10.1 and 11.10.2 of the Manual:

   (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.

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

11.10.9. Trust accounts

The AMLCO 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 Sections 11.10.1 and 11.10.2 of the Manual.

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.

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

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

1. The Company, in case where it offers the services of safekeeping of clients' funds and assets, may open "client accounts" (e.g. omnibus accounts) in the name of financial institutions from EEA countries or a third country which, in accordance with a relevant decision of the Advisory Authority it has been determined that the relevant third country which is defined by the Company as low-risk country, considering the para 3 of the Appendix 5.

   In that case the Company shall:

   i. Apply the measures and procedures referred to the Section 11.11 of this Manual;
   ii. ensure that the the third person is subject to mandatory professional registration in accordance with the relevant laws of the country of operation
   iii. Ensure that the third person is subject to regulation and supervision by an appropriate competent authority in the country of operation forAnti-Money Laundering and Terrorist Financing purposes

11.11. <u>Reliance on Third Persons for Client Identification and Due Diligence Purposes</u>

1. The Company may rely on third persons for the implementation of points (a), (b) and (c) of Client identification procedures and due diligence measures of Section 11.2 of the Manual, provided that:

   (a) The AMLCO ensures that the third person is an Obliged Entity, as provided in the Law, and gives their written approval for the collaboration; the written approval shall be kept in the third person's file.
   (b) 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

CySEC practices, that were collected in the course of applying Client identification and due diligence procedures

(c) 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 and suppression of Money Laundering and Terrorist Financing, according to the provisions of the Directive.

(d) the ultimate responsibility for meeting those requirements of Client identification and due diligence shall remain with the Company.

(e) The AMLCO keeps files/ records regarding third persons on which the Company relies on for the performance of KYC checks and due diligence procedures.

2. The Company does not rely on third parties established in high-risk third countries.

   It may be exempted from this prohibition a branch or majority owned subsidiary of the Company established in the European Union, where that branch or majority owned subsidiary fully complies with the group-wide policies and procedures in accordance with the provisions of section 68A of Law.

3. For the purposes of this Section of the Manual, ***third person*** means an obliged entity, as defined in Article 2A of the Law or an institution or person which is located in a member state or third country, and which:

   a) applies customer due diligence measures and record keeping measures which are consistent with the measures pursuant to the EU Directive; and is subject to supervision which is consistent with the relevant requirements of the EU Directive.

4. The Company must request from the third party to:

   (a) make immediately available data, information and documents obtained as a result of the application of the procedures establishing identity and customers due diligence measures in accordance with of points (a), (b) and (c) of Client identification procedures and due diligence measures of Section 11.2 of the Manual,

   (b) forward immediately to them, copies of these documents and relevant information on the identity of customer or the beneficial owner which the third party collected when applying the above procedures and measures.

5. 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 its 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.

6. In the case where the Company relies on a third person, shall apply the following additional measures/procedures:

   (a) Before the commencement of the business relationship or the effecting of the one-off transaction, the Company needs to apply KYC procedures and due diligence measures in relation to the third party.
   (b) The Company enters into an agreement with the third party, defining the mutual obligations of each party.
   (c) A separate file with all relative information needs to be kept for each third party of the present provision.
   (d) 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 AMLCO.

The AMLCO shall be responsible for the implementation of the provisions mentioned in this Section of the Manual.

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

12. ON-GOING MONITORING PROCESS

12.1. General

The Company has a full understanding of normal and reasonable activity of its Clients as well as of their economic profile identify activities 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, according to point (g) of Section 6.2 and Section 13 of the Manual.

The constant monitoring of the Clients' activities is an imperative element in the effective controlling of the risk of Money Laundering and Terrorist Financing.

In this respect, the AMLCO 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.

12.2. Procedures

The procedures and intensity of monitoring Clients' activities 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 activities, 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 determine[2] 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.

[2]

(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.

(g) The data and information collected for each client shall be updated based on the client's risk categorisation. Respectively for ;

- Low-risk clients every 3 years;
- Medium-risk clients every 2; and
- High-risk clients every year

In any event the Company shall ensure that the clients are obliged to inform immediately the Company, in case of any changes on the provided data and information.

In case where the Company is intending to make an act which falls within the cases which may be approved by virtue of the provisions of the Sanctions and/or Restrictive Measures, it submits through the CO, before the execution of said action, a request for rejection or approval, towards UIS or towards the Credit Institution involved which shall forward to ACES depending on the case.

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

13.1. Reporting of Suspicious Transactions to the Unit

The Company, in cases where it detects a suspicious activity or there is an attempt of executing transactions which knows or suspects that are related to money laundering or terrorist financing, shall report, through the AMLCO its suspicion to the Unit in accordance with Section 6.2 and Section 13 of the Manual.

13.2. 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 3 of the Manual. The relevant list is not exhaustive nor it includes all types of transactions that may be used,

nevertheless it can assist the Company and its employees (especially the AMLCO and the Head of the Administration/Back-Office Department) in recognising the main methods used for Money Laundering and Terrorist Financing. The detection by the Company of any of the transactions contained in the said list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds, the nature and economic/business purpose of the underlying transaction, and the circumstances surrounding the particular activity.

3. In order to identify suspicious transactions the AMLCO shall perform the following activities:

- monitor on a continuous basis any changes in the Client's financial status, business activities, type of transactions etc
- monitor on a continuous basis if any Client is engaged in any of the practices described in the list containing examples of what might constitute suspicious transactions/activities related to Money Laundering and Terrorist Financing which is mentioned in Appendix 3 of this Manual.

Furthermore, the AMLCO 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 according to point (e) of Section 6.2 of the Manual. The said reports are archived by the AMLCO
- 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 AMLCO is evaluated on the Internal Evaluation Report according to point (f) of Section 6.2 of the Manual, which is also filed in a relevant file
- if, as a result of the evaluation described above, the AMLCO decides to disclose this information to the Unit, then he prepares a written report, which he submits to the Unit, according to point (g) of Section 6.2 and Section 13.4 of the Manual.
- if as a result of the evaluation described above, the AMLCO decides not to disclose the relevant information to the Unit, then he fully explain the reasons for his decision on the Internal Evaluation Report.

13.3. AMLCO's Report to the Unit

According to Circular C058, all the reports of the AMLCO of point (f) of Section 6.2 of the Manual should be prepared online on the web-application of the Unit and submitted to it, though the goAML reporting system.

After the submission of a suspicion report of point (f) of Section 6.2 of the Manual, 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, according to Section 48 of the Law, 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 of point (f) of Section 6.2 of the Manual, 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.

According to Section 26(2)(c) of the Law, the Unit may instruct the Company to refrain from executing or delay the execution of a Client's transaction without such action constituting a violation of any contractual or other obligation of the Company and its employees.

Furthermore, after the submission of a suspicion report of point (f) of Section 6.2 of the Manual, the Clients' accounts concerned as well as any other connected accounts are placed under the close monitoring of the AMLCO.

13.4. Submission of Information to the Unit

The Company shall ensure (see also Section 14 of the Manual) that in the case of a suspicious transaction investigation by the Unit, the AMLCO will be able to provide without delay the following information:

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

14. RECORD-KEEPING PROCEDURES

14.1. General

The Administration/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
(c) relevant correspondence documents with clients and other persons with whom a business relationship is maintained.
(d) relevant information for each third party which the Company relies on for client identification and due diligence procedures.

The documents/data mentioned above shall be kept for a period of at least five (5) 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.

Any data or records maintain from automated screening database, shall be ensured that is up to date and correct.

14.2. Format of Records

The Administration/Back-Office Department may retain the documents/data mentioned in Section 14.1 of the 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 Administration/Back-Office Department shall be able to retrieve the relevant documents/data without undue delay and present them at any time, to CySEC or to the Unit, after a relevant request.

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

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

14.3. Certification and language of documents

1. The documents/data obtained, shall be in:
    i. original or
    ii. certified true copy of original, where certification is made by the Company, in case it makes itself the KYC verification, and original documented is presented ;
    iii. , certified true copy or original in the case that the documents/data are certified as true by a third person as described in Section 11.11 or;

iv. Notarized/apostilled, in the case where certification is made by the competent authority or person, which according to the relative laws of their country, are responsible for the certification of authenticity of the documents or evidence.

v. Given that at least one of the procedures mentioned in paragraph 11.9.1.(d) of the Manual, in relation to non-face-to-face clients:

- Copy of the original or
- Electronic form, subject to the para 2 below:

2. Perform due diligence procedure by electronic means:

i. The verification of the identity is performed either by the Company or by a third party. Both shall apply the following provisions:

- The electronic databases maintained by the third party or to which the third party or the Company have access, shall be registered or approved by the Commissioner of Personal Data Protection (or the relevant competent authority in the country of keeping of said data bases).
- The electronic data bases provide access to information related to both current and past statuses of the person, indicating its real existence, and contain both positive information (at least full name, address and date of birth), as well as negative (for ex. commission of crimes such as ID stealing, inclusion in lists of deceased persons, inclusion in sanctions lists and restrictive measures by the Council of the EU and the UN Security Council).
- The databases shall contain a wide range of sources with information from various time intervals, which are updated in real-time and send trigger alerts when important data/information is amended.
- They shall apply transparent procedures that allow the Company to know the information investigated, the results, and their importance in relation to the degree certainty as to the identity of the Client.
- They shall establish procedures which allow the Company to record and keep the information used, and the results in relation to the Client's identity.

ii. The data/information shall be derived from two or more sources. The following provisions, shall be applied at minimum, for fulfilling the identity by electronic means:

- Locate the full name and the current resident address of the Client, from a single source; and
- Locate the full name or the current resident address or the date of birth of the Client, from a second source.

iii. For identifying the Client by electronic means, the Company has in place procedures which satisfy the completeness, validity and reliability of the data/information that it has access. The checking procedure must include investigation for both positive and negative information.

iv. The Company shall assess the results for the Client's identity in such basis in order to fulfil the provisions of Section 11.6, para. 3 of this Manual. The Company shall establish adequate mechanisms in order to assess the quality of the data/information.

3. A true translation shall be attached in the case that the documents of point (1) above are in a language other than Greek of English.

Each time the Company shall proceed with the acceptance of a new Client, the Head Administration/Back-Office Department shall be responsible for ensuring compliance with the provisions of points 1 and 2 above.

15. EMPLOYEES' OBLIGATIONS, EDUCATION AND TRAINING

15.1. 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, according Section 6.2, 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.

15.2. Education and Training

15.2.1. Employees' Education and Training Policy

(a) The Company shall ensure that its employees are fully aware of their legal obligations according to the Law and the Directive, as well as internal policies and procedures including unique risks the Company may face, by introducing a complete employees' education and training program
(b) The employees shall receive training with regards to their legal obligation to report on any reasonable suspicion or knowledge that comes to their attention that another person is engaged in laundering or financing of terrorism offences. In such cases, employees are obliged to make an internal report to the AMLCO. Moreover, the employees shall receive on-going training with regards to suspicious activity monitoring and reporting, and specifically with regards to the recognition and handling of transactions and activities which may be related to money laundering or terrorist financing.
(c) 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. Such content shall be reviewed and updated on a regular basis to ensure that it remains current and appropriate and the material is approved by senior management. Enhanced training shall be provided to senior management and staff in key AML/FT roles. 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 of the Republic including any relevant acts of the European Union.
(d) Training may take many forms and may include: face-to-face training seminars, completion of online training sessions, attendance at AML/FT conferences and

participation in dedicated AML/FT forums, practice group meetings for discussion of AML/FT issues and risk factors, guidance notes, newsletters and publications on current AML/FT issues.

(e) the training program aims at educating the Company's employees on the latest developments in the Prevention and Suppression of Money Laundering and Terrorist Financing, including the practical methods and trends used for this purpose

(f) 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 new developments.

(g) Training shall be provided to staff prior to commencing work and at minimum on an annual basis. The Company shall establish mechanisms to facilitate prompt updates on key trends, emerging risks, potential ML/TF activities/risks, legislative changes and internal policies, controls and procedures and shall ensure that such updates are communicated to staff in a timely manner.

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. Training records shall be maintained.

The Company shall assess the adequacy and effectiveness of the conducted training, by introducing tests following the completion of each training session.

15.2.2. AMLCO Education and Training Program

The *Senior Management* of the Company shall be responsible for the AMLCO of the Company to attend external training. Based on his/her training, the AMLCO will then provide training to the employees of the Company further to Section 15.2.1 above.

The person to be appointed as AMLCO must possess the relevant certification mentioned in subparagraph 5.5 of Directive R.A.D. 44/2019, as amended) of CySEC.

The main purpose of the AMLCO training is to ensure that relevant employee(s) become aware of:

- the Law and the Directive
- 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
- the importance of the Clients' due diligence and identification measures requirements for money laundering prevention purposes.

The AMLCO 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.

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 the Client.

3. The transactions or the size of the transactions requested by the Client do not comply with his usual practice and business activity.

4. Large volume of transactions and/or money deposited or credited into, an account when the nature of the Client's business activities would not appear to justify such activity.

5. The Business Relationship involves only one transaction, or it has a short duration.

6. There is no visible justification for a Client using the services of a particular obligated entity. For example the Client is situated far away from the particular obligated entity and in a place where he could be provided services by another obligated entity.

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 Terrorist Financing.

15. A Client is reluctant to provide complete information when establishes a Business Relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with obligated entity, 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 obligated entity 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 obligated entity, 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 obligated entity.

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 the Law 144/(I)/2007, Third Appendix, Part I or the administrative services provided in accordance to Law 196(I)/2012, Article 4(1)(a)(b)			
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 MOKAS			
L.	Reasoning if related internal suspicious reports and/or reports to MOKAS 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)			

APPENDIX 5

Non-exhaustive list of factors and types of evidence of potentially lower risk:

(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) clients that are resident in geographical areas of lower risk as set out in point (3) below;

(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 and the policy cannot be used as collateral;

(c) a pension 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 services to 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 managed by other factors such as purse limits or transparency of ownership such as certain types of electronic 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.

APPENDIX 6

Non-exhaustive list of factors and types of evidence of potentially higher risk:

(1) Customer risk factors:
- (a) the business relationship is conducted in unusual circumstances;
- (b) clients that are resident in geographical areas of higher risk as set out in point (3) below;
- (c) legal persons or arrangements that are personal asset-holding vehicles;
- (d) companies that have nominee shareholders or shares in bearer form;
- (e) businesses that are cash-intensive;
- (f) the ownership structure of the company appears unusual or excessively complex given 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 un-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) without prejudice to Article 64(1)(a) of the Law, 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.

APPENDIX 7

High-Risk Countries

High-Risk third countries are those as identified and published from time to time via relevant public statements, regulations reports etc. by the Financial Action Task Force and the European Commission.

Below are the links that should be reviewed regarding high-risk jurisdictions:

https://aml-cft.net/library/basel-aml-index/
https://www.knowyourcountry.com/country-ratings-table
https://www.fatf-gafi.org/countries/
http://www.fatf-gafi.org/countries/#high-risk

APPENDIX 8

Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849

Remote Customer Onboarding (identification process) Guidelines

Scope

These guidelines apply when performing the initial customer due diligence (CDD) to onboard new customers, using remote channels, without physical contact.

Definitions

Digital Identity: A material or immaterial unit that contains person identification data, which is used to verify the identity of the user and for authentication purposes in an online service.

Digital Identity Issuer: A third party trusted with the assessment and verification of the authenticity of the credentials or attributes which will serve as basis for the customer's identification.

Biometric data: Personal data relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Impersonation Fraud Risk: The risk that the customer uses another person's (natural or legal) details without the consent or knowledge of the person whose identity is being used.

Acquisition of information

1. Identifying the customer

Where the Company do not resort to digital identity issuers to identify the customer should ensure that:

a) the information obtained through the remote customer onboarding solution is up-to-date and adequate to meet the standards for initial customer due diligence;

b) any images, video, sound and data are captured in a readable format and with sufficient quality so that the customer is unambiguously recognisable;

c) the images, video, sound and data are stored according to GDPR Regulation18 and remain available to the Company;

d) any technical shortcomings that might hinder the identification process, such as unexpected connection interruptions, are detected and investigated.

The identification proofs collected during the remote identification process, which are required to be retained in accordance with Article 40(1) point (a) of Directive (EU) 2015/849, should be time-stamped and stored securely. The content and the quality of stored records, including pictures and videos, should be available in a readable format and allow for ex-post verifications.

1.1 Identifying Natural Persons

Detailed below are the typical and acceptable documents for confirming a client's identification and address. One document cannot be used as evidence for both ID and address. All documents provided **must** be clear and legible.

Account Type	Acceptable evidence of Identification	Acceptable evidence of address
Individual or jointly held accounts. (For joint accounts evidence is required for each joint holder)	> A current (within 6 months of expiry) photograph bearing passport > National Identity Card > A current (within 6 months of expiry) photograph bearing drivinglicense > EEA member state identity card > Residence permit issued by the Home Office to EEA nationals onsight of own country passport	> A utility, gas, electric, water or telephone landline, rates or council bill dated within 3 months > A state pension or government benefits book > A tax assessment document > A bank or bank credit card statement dated within 3 months > Proof of home ownership or a rental agreement or a mortgage statement > A current (within 6 months of expiry) photograph bearing driving license

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. A person's residential and business address will be an essential part of his identity.
A screen shot of the client holding up the POI next to their face should be taken.

1.2 Identifying Legal Entities

Where the Company remotely onboard customers that are legal entities, the same data and information issued or obtained as described in Section 11.6 of this manual.

The Company should ensure that collects:

a) all relevant data and documentation to identify and verify the legal person and to verify that the natural person they are dealing with is legally entitled to act on behalf of the legal entity;

b) the information regarding the beneficial owners in accordance with this manual

For the natural persons who are acting on behalf of legal persons, financial sector operators should apply the identification process described in the Section 1.1 above.

1.3 Nature and purpose of the business relationship

The Company should obtain information on the purpose and intended nature of the business relationship. The Company should gather information from their customers to identify the nature of their personal, professional or business activities and expected source of funds, and verify the accuracy of this information as necessary.

1.4 Document Authenticity & Integrity

Where the Company accept paper copies, photos or scans of paper-based documents in the course of remote customer onboarding without having the possibility to examine the original identification document, they should verify the following:

a) if the copy, photo or scan reproduces security features embedded in the original document and if the specifications of the original document that are being reproduced by the copy are valid and acceptable, in particular, type, size of characters and structure of the document, by comparing them with official databases.

b) that no alteration of the personal data in the document has been attempted;

c) the integrity of the algorithm used to generate the unique identification number of the original document; in case the official document has been issued with machine-readable zone (MRZ);

d) that the copy, photo or scan of the identification document is of sufficient quality and definition so as to ensure that relevant information is unambiguous;

e) where applicable, that the picture of the customer embedded in the document was not replaced.

Where the Company accepts alternative documentation should carry out additional controls or increase human intervention to verify the reliability of non-traditional forms of identity documentation.

1.5 Authenticity Checks

The Company should be able, as a minimum, to verify the validity of official documents issued by a public authority as part of the remote verification process to ensure:

a) that the identity of the customer coincides with the person previously identified, in cases of natural persons;

b) that the legal entity has the right to conclude contracts and it is established in its respective jurisdiction;

c) the natural person that represents a legal entity is entitled to act on behalf of such entity.

Where the remote customer onboarding solution involves the use of biometric data to verify the customer's identity, the Company should make sure that the biometric data have enough uniqueness to be unequivocally referable to a single natural person. The Company should verify the unambiguous match between the biometric data indicated on the submitted identity document and the customer being onboarded.

Where the ML/TF risk associated with a business relationship is increased, the Company should use remote verification processes that include liveness detection procedures

examining whether the video, picture or other biometric data captured during the remote customer onboarding process belong to a living person present at the point of capture, or real-time videoconference.

In case of legal entities, the Company should verify the identity and the information provided in the documents and attributes reviewed as part of the identification process, through a reliable and independent source of information such as public registers, where available.

In situations where the evidence provided is of insufficient quality resulting in ambiguity or uncertainty so that the performance of remote checks is affected, the individual remote customer onboarding process should be discontinued and redirected, where possible, to a face-to-face verification, in the same physical location.

a) ensure that the photograph(s) is taken under proper lighting conditions and that the required properties are captured with absolute clarity;

b) ensure that the photograph(s) is taken at the time the customer is performing the verification process. This may be achieved by using a dynamic photograph, multiple photo shots under different angles or another similar method;

c) perform liveness detection verifications, which may include procedures where a specific action from the customer to verify that he/she is present in the communication session, or it can be based on the analysis of the received data and does not require an action by the customer;

Where the Company use photograph(s) as a mean to verify the identity of the customer by comparing it with a picture(s) incorporated in an official document, they should:

d) in the absence of human verification, use strong and reliable algorithms to verify if the photograph(s) taken match with the pictures retrieved from the official document(s) belonging to the customer or representative.
e) ensure that the quality of the image and audio is sufficient to allow the proper verification of the customer's identity and that reliable technological systems are used;

Where the Company use a video conference as a mean to verify the identity of the customer, should:

a) ensure that the quality of the image and audio is sufficient to allow the proper verification of the customer's identity and that reliable technological systems are used;

b) foresee the participation of staff that has sufficient knowledge of the applicable AML/CFT regulation and security aspects of remote verification and who is sufficiently trained to anticipate and prevent the intentional or deliberate use of deception techniques related to remote verification, and to detect and react in case of their occurrence;

c) develop an interview guide defining the subsequent steps of the remote verification process as well as the actions required from the employee. The interview guide should include guidance on observing and identifying psychological factors or other features that might characterise suspicious behaviour during remote verification.

Where possible, the Company should use remote customer onboarding solutions that include randomness in the sequence of actions to be performed by the customer for verification purposes. It should also provide random assignments to the employee responsible for the remote verification process to avoid collusion between the customer and the responsible employee.

In addition to the above, and where appropriate to the ML/TF risk presented by the business relationship, the Company should use of one or more of the following controls:

a) the first payment is drawn on an account in the sole or joint name of the customer with an EEA-regulated credit or financial institution or in a third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849;

b) send a randomly generated passcode to the customer to confirm the presence during the remote verification process. The passcode should be a single-use and time-limited code;

c) capture biometric data to compare them with data collected through other independent and reliable sources;

d) telephone contacts with the customer;

e) direct mailing (both electronic and postal) to the customer.


HOLBORN