



EVERYTHING YOU NEED AND MORE

Holiway Investments Ltd
Address: 30, Tempon Street, Egkomi, CY-2408 Nicosia
Licence Number: 248/14 **Licence Date:** 10/10/2014
Obligated Entity Registration Number: 325316 **Telephone:**
22 35 35 57 **Fax:** 22 000 513
Domain : www.10tradeFX.eu ;
www.miltonprime.eu ;

HOLIWAY INVESTMENTS LIMITED

ANTI-MONEY LAUNDERING AND COMBATTING THE TERRORIST OF FINANCING MANUAL

NOVEMBER 2020 UPDATE



EVERYTHING YOU NEED AND MORE

Holiway Investments Ltd

Address: 30, Tempon Street, Egkomi, CY-2408 Nicosia

Licence Number: 248/14 **Licence Date:** 10/10/2014

Obligated Entity Registration Number: 325316 **Telephone:**

22 35 35 57 **Fax:** 22 000 513

Domain : www.10tradeFX.eu ;

www.miltonprime.eu ;



EVERYTHING YOU NEED AND MORE

Contents

General Definitions	8
1. Range of Application.....	12
1.1. Introduction	12
1.2 Purpose	12
1.3. Scope	12
1.4. Application	13
2. Responsibilities of the Board of Directors.....	13
2.1 General Responsibilities	13
3. Responsibilities of the Internal Audit Function.....	14
3.1 General Responsibilities	14
4. The Money Laundering Compliance Officer	14
4.1 General Responsibilities	14
4.2 Duties of the MLCO.....	15
5. The Annual Report of the MLCO.....	17
5.1 Scope of the Report	17
5.2 Content of the Report & Areas Covered.....	18
6. Monthly Prevention Statement	19
6.1 Ongoing Regulatory Reporting.....	19
7. Risk Based Approach	20
7.1 Approach Outline	20
7.2 Measures & Procedures	20
7.3 Identification of Risks	21
7.4 Design and Implementation of Measures and Procedures to Manage and Mitigate Risks	22
7.5 Dynamic Risk Management	23
7.6 Relevant International Organizations	23
8. Client Acceptance Policy.....	24
8.0 General Principles of the CAP	24
8.1 Criteria for Accepting New Clients (based on their respective risk)	24
8.1.1 Low Risk Clients	24

EVERYTHING YOU NEED AND MORE

8.1.2 Normal Risk Clients.....	24
8.1.3 High Risk Clients.....	24
8.1.4 Not Acceptable Clients.....	24
8.2 Client Categorization Criteria.....	25
8.2.1 Low Risk Clients.....	25
8.2.2 Normal Risk Clients.....	26
8.2.3 High Risk Clients.....	26
9. Client Due Diligence & Identification Procedures.....	26
9.1 Application of Procedures.....	26
9.2 Open a new client account.....	27
9.2.1 Physical Persons accounts.....	28
9.2.2 Proof of Identity.....	28
9.2.3 Proof of Address.....	31
9.2.4 Legal persons account.....	31
9.2.5 Accounts maintenance.....	32
9.3 Ways of Application of Client Identification and Due Diligence Procedures.....	33
9.4 Transactions that Favor Anonymity.....	34
9.5 Failure or Refusal to Submit Information for the Verification of Clients' Identity.....	35
9.6 Time of Application of the Client Identification and Due Diligence Procedures.....	35
9.7 Construction of Economic Profile, Client Identification & Due Diligence Principles.....	36
9.8 Further Obligations for Client Identification and Due Diligence Procedures.....	38
9.9 Simplified Client Identification and Due Diligence Procedures.....	39
9.10 Enhanced Client Identification and Due Diligence (High Risk Clients).....	40
9.11 Non face-to-face Clients.....	41
9.12 Account in names of companies whose shares are in bearer form.....	42
9.13 Trust accounts.....	43
9.14 'Client accounts' in the name of a third person.....	43
9.15 "Politically Exposed Persons" accounts.....	44
9.16 Electronic gambling & gaming through the internet.....	47
9.17 Clients from high risk third countries.....	48
9.18 Clients from countries which inadequately apply FATF's recommendations.....	49
9.19 Client Identification and Due Diligence Procedures (Specific Cases).....	50



EVERYTHING YOU NEED AND MORE

9.20	Natural persons residing in the Republic.....	50
9.21	Natural persons not residing in the Republic.....	51
9.22	Joint accounts	51
9.23	Accounts of unions, societies, clubs, provident funds and charities.....	51
9.23	Accounts of unincorporated businesses, partnerships and persons with no legal substance	52
9.24	Accounts of legal persons.....	52
9.25	Investment funds, mutual funds and firms providing financial or investment services	54
9.26	Nominees or agents of third persons	55
9.27	Reliance on Third Persons for Client Identification and Due Diligence Purposes	55
10.	On Going Monitoring	58
10.1.	General	58
10.2.	Procedures	58
11.	Recognition & Reporting Of Suspicious Transactions /Activities To The Unit.....	61
11.1	Reporting of Suspicious Transactions to the Unit	61
11.2	Suspicious Transactions	61
11.3	MLCO's Report to the Unit.....	62
11.4	Submission of Information to the Unit	63
12.	Record-Keeping Procedures	63
12.1	General	63
12.2	Format of Records	64
12.3	Certification and language of documents	64
12.4	True Translation	67
13.	Employees' Obligations, Education And Training.....	67
13.1	Employees' Obligations	67
13.2	Education and Training	68
13.3	MLCO Education and Training Program	68
14.	FATCA & CRS Reportable Information: General Requirements	69
15.	General Data Protection	70
	Appendix I.....	71



EVERYTHING YOU NEED AND MORE

INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING	71
Appendix II.....	72
INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING	72
Appendix III	73
Examples of Suspicious Transactions/Activities Related To Money Laundering And Terrorist Financing	73
Appendix IV	
Banned Jurisdictions.....	78



EVERYTHING YOU NEED AND MORE

Holiway Investments Ltd
Address: 30, Tempon Street, Egkomi, CY-2408 Nicosia
Licence Number: 248/14 **Licence Date:** 10/10/2014
Obligated Entity Registration Number: 325316 **Telephone:**
22 35 35 57 **Fax:** 22 000 513
Domain : www.10tradeFX.eu ;
www.miltonprime.eu ;

Abbreviations used in this manual:

AML	Anti-Money Laundering
CAP	Client Acceptance Policy
CDD	Client Due Diligence
CFT	Combatting Financing of Terrorism
CIF	Cyprus Investment Firm
CySEC	Cyprus Securities and Exchange Commission
EEA	European Economic Area
FATF	Financial Action Task Force
MLCO	Money Laundering Compliance Officer
ML&TF	Money Laundering and Terrorist Financing
PEP's	Politically Exposed Persons

General Definitions

“**Advisory Authority**” means the Advisory Authority for Combating Money Laundering and Terrorist Financing which is established under Section 56 of the Law.

“**Beneficial Owner**” means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted and includes at least:

The Beneficial Owner shall at least include:

(a) in the case of corporate entities:

i. the natural person or natural persons, who ultimately own or control a legal entity through direct or indirect ownership or control a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, or through control via other means, other than a Obligated Entity listed on a regulated market that is subject to disclose requirements consistent with Union law or subject to equivalent international standards which ensure adequate transparency of ownership information.

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

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

iii. The natural person or natural persons, may be the person who hold the position of senior managing official, provided that all the requirements stated in the said definition are met.

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

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



EVERYTHING YOU NEED AND MORE

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

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

“Obligated Entity” means HOLIWAY INVESTMENTS LTD which is incorporated in the Republic of Cyprus with registration number HE325316.

“Directive” means the Prevention of Money Laundering and Terrorist Financing Directive DI144-2007-08, as amended, of the Cyprus Securities and Exchange Commission.

“European Economic Area (EEA)” means Member State of the European Union or any 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 the Directive 2005/60/EC of the European Parliament and the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of Money Laundering and Terrorist Financing

“Investment and Ancillary Services” means the investment and ancillary services as per Part I and II of the Third Appendix of the Law 144(I)/2007, as amended, for which the Obligated Entity is licensed by the Cyprus Securities and Exchange Commission to offer.

“Law” means The Prevention and Suppression of Money Laundering Activities Law; Law 188(I)/2007, 58(I)/2010, 80(I)/2012, 192(I)/2012, 101(I)/2013.

“Manual” means the Anti-Money Laundering and Combatting Financial Crime Manual (this manual), according to the Directive.

“Money Laundering and Terrorist Financing” means the money laundering offences and terrorist financing offences defined in Section 2 of the Law, referred to also the following.

Every person who (a) knows or (b) at the material time ought to have known that any kind of property constitutes proceeds from the commission of a predicate offence as this is defined in Section 2 of the Law, 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;

EVERYTHING YOU NEED AND MORE

- (iv) (iv) participates in, associates, co-operates, conspires to commit, or attempts to commit and aids and abets and provides counselling or advice for the commission of any of the offences referred to above;
- (v) provides information in relation to investigations that are carried out for laundering offences for the purpose of enabling the person who acquired a benefit from the commission of a predicate offence to retain the proceeds or the control of the proceeds from the commission of the said offence; and
- (vi) commits an offence punishable by fourteen years' imprisonment or by a pecuniary penalty of up to €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 €50.000 or by both in the case of (b) above.

“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 Obligated Entity 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 Obligated Entity, 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 Obligated Entity, 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, and
- (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 Persons (PEPs)” means the natural persons who are or have been entrusted with prominent public functions (see below) in the Republic or in any another country and their immediate family members or persons known to be close associates of such persons:

- (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,



EVERYTHING YOU NEED AND MORE

the decisions of which are not subject to further appeal, except in exceptional circumstances;

- (e) Members of courts or auditors or of the boards of central banks;
- (f) Ambassadors, charges 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 or equivalent function of an international organization
- (i) Members of the governing bodies of political parties;
- (j) Mayors;

No public function referred to in points (a) to (j) of the respective directive shall be understood as covering middle-ranking or more junior officials;

“**Republic**” means the Republic of Cyprus.

“**Regulated Market**” means a multilateral system managed or operated by a market operator and which brings together or facilitates the bringing together of multiple third-party buying or/and selling interests in financial instruments - in the system and in accordance with its non- discretionary rules - in a way that results in a contract, in respect of the financial instruments admitted to trading under its rules or/and systems, and which is authorized and functions regularly in accordance with the provisions of Part X of Law 144(I)/2007, as amended, or respective legislation of other member states that are enacted in compliance with Directive 2004/39/EC.

“**Shell Bank**” means a credit institution or an institution engaged in equivalent activities to those carried out by credit institutions and financial institutions, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

“**Third Country**” means a 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.

“**High Risk third Country**” means a third country, designated by the Commission pursuant to the provisions of section 9 (2) of the Directive of the EU by the issuance of acts by way of derogation, which presents strategic 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 categorized by the Obligated Entity as high risk in accordance with the risk assessment foreseen by section 58A.

“**Senior Management**” the person that holds the position of the senior management official may be a member of the Board of Directors as well, however it is not a requirement.

1. Range of Application

1.1. Introduction

HOLIWAY INVESTEMENTS LTD (hereafter the “Obligated Entity”) is a Cypriot investment firm established in accordance with the laws of the Republic of Cyprus and is regulated by the Cyprus Securities and Exchange Commission (hereafter “CySEC”) with license number 248/14. This document represents the Obligated Entity’s Anti-Money Laundering and Combatting the Financing of Terrorism Manual (“AML & CFT”) which is based on the 4th Anti-Money Laundering Directive (EU).

1.2 Purpose

The purpose of the Manual is to lay down the Obligated Entity’s internal practices, measures, procedures and controls relevant to the prevention of Money Laundering and Terrorist Financing.

The Manual is developed and periodically updated by the MLCO based on the general principles set up by the Obligated Entity’s Board of Directors (the “Board”) in relation to the prevention of Money Laundering and Terrorist Financing.

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

The Manual shall be communicated by the MLCO to all the employees of the Obligated Entity that manage, monitor or control in any way Clients’ transactions and have the responsibility for the application of practices, measures, procedures and controls that have been determined herein.

The Manual has been prepared to comply with the all provisions of the Law, and relative Directives of the CySEC.

1.3. Scope

This document complements, but does not replace:

- the Internal Procedures Manual of the Obligated Entity;
- all relevant Obligated Entity policies, including the Key Operating Policies;
- any publications referenced within the Manual.

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

1.4. Application

The Manual applies to all the services offered to the Obligated Entity’s Clients as well as the relevant Obligated Entity’s dealings with its Clients, including but not limited to trading in

EVERYTHING YOU NEED AND MORE

CFD(s) and foreign exchange trading transactions, which either do not aim to physically deliver the agreed foreign currency or are not materially settled in cash (foreign exchange spot trading), irrespective of the Client account size and frequency of trading.

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

2. Responsibilities of the Board of Directors

2.1 General Responsibilities

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

- (a) to determine, record and approve the general policy principles of the Obligated Entity in relation to the prevention of Money Laundering and Terrorist Financing and communicate them to the MLCO;
- (b) to appoint a senior official that possesses the skills, knowledge and expertise relevant to financial and other activities depending on the situation, who shall act as the MLCO and where necessary, assistant MLCO's and determine their duties and responsibilities, which are recorded in this Manual;
- (c) to approve the Manual;
- (d) to ensure that all requirements of the Law and the Directive are applied, and assure that appropriate, effective and sufficient systems and controls are introduced for achieving the abovementioned requirements;
- (e) to ensure that the MLCO and his assistants, if any, and any other person who has been assigned with the duty of implementing procedures for the prevention of Money Laundering and Terrorist Financing (i.e. Administration/Back-Office Department personnel), have complete and timely access to all data and information concerning Clients' identities, transactions' documents (as and where applicable) and other relevant files and information maintained by the Obligated Entity so as to fully facilitate in the effective execution of their duties, as included herein;
- (f) to ensure that all employees are aware of the person who has been assigned as the MLCO, as well as his assistants (if any), to whom they report any information concerning transactions and activities for which they have knowledge or suspicion that might be related to Money Laundering and Terrorist Financing;
- (g) to establish a clear and efficient reporting chain based on which information, regarding suspicious transactions is passed without delay to the MLCO, either directly or through his assistants, if any, and notifies accordingly the MLCO for its explicit prescription in the Manual;
- (h) to ensure that the MLCO, the assistant MLCOs, if any, and the Administration/Back-

Office Department have sufficient resources, including competent staff and technological equipment, for the effective discharge of their duties;

EVERYTHING YOU NEED AND MORE

- (i) to assess and approve the MLCO's Annual Report and take all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the abovementioned report; and
- (j) to meet and decide the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected in the Internal Auditor's report. The minutes of the said decision of the Board and the Internal Auditor's report shall be submitted to CySEC within twenty (20) days from the said Board meeting and no later than four (4) months after the end of the calendar year (i.e. the latest, by the end of April each year).
- (k) To periodically review of the general principles of the employees Access Levels policy and its implementation.

3. Responsibilities of the Internal Audit Function

3.1 General Responsibilities

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

- (a) the Internal Auditor shall review and evaluate, at least on an annual basis, the appropriateness, effectiveness and adequacy of the policy, practices, measures, procedures and control mechanisms applied for the prevention of Money Laundering and Terrorist Financing mentioned in the Manual; and
- (b) the findings and observations of the Internal Auditor, in relation to point (a) above, shall be submitted, in a written report form to the Board.

4. The Money Laundering Compliance Officer

4.1 General Responsibilities

The MLCO shall always be a senior official that possesses the skills, knowledge and expertise relevant to financial and other activities depending on the situation, so as to command the necessary authority. Furthermore, the MLCO shall lead the Obligated Entity's Money Laundering Compliance procedures and processes and report to the Senior Management.

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

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

In performing his role, the MLCO shall take into account the nature, scale and complexity of the Obligated Entity's business, and the nature and range of investment services and activities undertaken in the course of the business.

4.2 Duties of the MLCO

During the execution of his duties and the control of the compliance of the Obligated Entity with the Law and the Directive, the MLCO shall obtain and utilize data, information and reports

issued by international organizations, as stated in Section 7.6 of the Manual.

The duties of the MLCO and the alternate MLCO shall include, inter alia, the following:

- (a) to design, based on the general policy principles of the Obligated Entity mentioned in point 2.1(a) of Section 2 of the Manual, the internal practices, measures, procedures and controls relevant to the prevention of Money Laundering and Terrorist Financing, and describe and explicitly allocate the appropriateness and the limits of responsibility to each department that is involved in the abovementioned;

It is provided that, the above includes 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 the daily activities of the Obligated Entity with regard to the development of new products and possible changes in the Obligated Entity's economic profile;

- (b) to develop and establish the CAP according to Section 8 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 policy mentioned in point 2.1(a) of Section 2 of the Manual, the practices, measures, procedures and controls of point (a) above and in general the implementation of the Manual. In this respect, the MLCO shall apply appropriate monitoring mechanisms (e.g. on-site visits to departments of the Obligated Entity) which will provide him with all the necessary information for assessing the level of compliance of the departments and employees of the Obligated Entity with the procedures and controls which are in force; In the event that the MLCO identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, gives appropriate guidance for corrective measures and where deems necessary informs the Board;
- (e) to receive information from the Obligated Entity'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 found in Appendix I of the Manual;
- (f) to evaluate and examine the information received as per point (e) above, by reference to other relevant information and discuss the circumstances of the case with the informer and where appropriate, with the informer's superiors.
The evaluation of the information of point (e) above shall be done on a report (hereinafter the "Internal Evaluation Report"), a specimen of such report is found in Appendix II of the Manual;
- (g) if following the evaluation described in point (f) above, the MLCO decides to notify the Money Laundering Combat Unit of the Republic (the "Unit"), then he shall

EVERYTHING YOU NEED AND MORE

complete an XML electronic report and submit it to the Unit at the soonest possible through the goAML IT system, a specimen of the goAML site.

- (h) It is provided that, after the submission of the MLCO Report to the Unit, the accounts involved and any other connected accounts, are closely monitored by the MLCO and following any directions from the Unit, thoroughly investigates and examines all the transactions of the accounts, as applicable and relevant to the Investment and Ancillary Services;
- (i) to act as a first point of contact with the Unit, upon commencement of and during any investigations as a result of filing a report to the Unit according to point (g) above;
- (j) to ensure the preparation and maintenance of the lists of Clients categorised following a risk-based approach, which contains, among others, the names of Clients, their account number and the dates of the commencement of the Business Relationship. Moreover, the MLCO ensures the updating of the said list with all new or existing Clients, in light of any additional information obtained;
- (k) to detect, record, and evaluate, at least on an annual basis, all risks arising from existing and new Clients, new financial instruments and services and update and amend the systems and procedures applied by the Obligated Entity for the effective management of the aforesaid risks;
- (l) to evaluate the systems and procedures applied by any third persons on whom the Obligated Entity may rely on for Client identification and due diligence purposes, according to Section 9.26 of the Manual, and approve the cooperation with said third persons;
- (m) to ensure that the branches and subsidiaries of the Obligated Entity, if any, that operate in countries outside the EEA, have taken all necessary measures for achieving full compliance with the provisions of the Manual, in relation to Client identification, due diligence and record keeping procedures;
- (n) to provide advice and guidance to employees of the Obligated Entity on subjects related to money laundering and terrorist financing;
- (o) to acquire the knowledge and skills required for the improvement of the appropriate procedures for recognizing, preventing and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing;
- (p) to determine whether the Obligated Entity's departments and employees that need further training and education for the purpose of preventing Money Laundering and Terrorist Financing and organizes appropriate training sessions/seminars. In this respect, the MLCO prepares and applies an annual staff training program according to Section 13.2 of the Manual. Also, the MLCO assesses the adequacy of the education and training provided;
- (q) to prepare correctly and submit timely to CySEC the monthly prevention statement of Section 6 of the Manual and provide the necessary explanation to the appropriate employees of the Obligated Entity for its completion; to respond to all requests and queries from the Unit and CySEC, to provide all requested information and fully cooperate with the Unit and CySEC; and
- (r) to maintain a registry which includes the reports of points (e), (f) and (g), and relevant

EVERYTHING YOU NEED AND MORE

statistical information (e.g. the department that submitted the internal report, date of submission to the MLCO, 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.

5. The Annual Report of the MLCO

5.1 Scope of the Report

The Annual Report of the MLCO is a significant tool for assessing the Obligated Entity's level of compliance with its obligations as laid down in the Law and the Directive.

The MLCO's Annual Report shall be prepared and submitted to the Board for approval within two months from the end of each calendar year (i.e. at 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. at 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.

5.2 Content of the Report & Areas Covered

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 MLCO, reporting the material deficiencies and weaknesses identified in the policy, practices, measures, procedures and controls that the Obligated Entity applies for the prevention of Money Laundering and Terrorist Financing. In this respect, the report outlines the seriousness of the deficiencies and weaknesses, the risk implications and the actions taken and/or recommendations made for rectifying the situation;
- (c) the number of Internal Suspicion Reports submitted by Obligated Entity personnel to the MLCO, according to point (e) of Section 4.2 of the Manual and possible
- (d) comments/observations thereon;
- (e) the number of reports submitted by the MLCO to the Unit, according to point (g) of Section 4.2 of the Manual with information/details on the main reasons for suspicion and highlights of any particular trends;
- (f) information, details or observations regarding the communication with the employees on money laundering and terrorist financing preventive issues;

EVERYTHING YOU NEED AND MORE

- (g) summary figures, on an annual basis, of Clients' total cash deposit in Euro and other currencies in excess of the set limit of €10.000 (together with comparative figures for the previous year) as reported in the monthly prevention statement of Section 6 of the Manual. Any comments on material changes observed compared with the previous year are also reported;
- (h) information on the policy, measures, practices, procedures and controls applied by the Obligated Entity 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;
- (i) information on the systems and procedures applied by the Obligated Entity for the ongoing monitoring of Client accounts and transactions;
- (j) information on the measures taken for the compliance of branches and subsidiaries of the Obligated Entity, 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;
- (k) information on the training courses/seminars attended by the MLCO and any other educational material received;
- (l) 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;
- (m) results of the assessment of the adequacy and effectiveness of staff training;
- (n) information on the recommended next year's training program; and
- (o) information on the structure and staffing of the department of the MLCO 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.

6. Monthly Prevention Statement

6.1 Ongoing Regulatory Reporting

The MLCO shall prepare and submit to CySEC, according to point (q) of Section 4.2 of the Manual, on a monthly basis, the CySEC Form 144-08-11 "Monthly Prevention Statement regarding the prevention of Money Laundering and Terrorist Financing", which includes details as regards the total cash deposits accepted by the Obligated Entity, the Internal Suspensions Reports, and the MLCO's Reports to the Unit, according to points (e) and (g) in Section 4.2 of the Manual, respectively.

The aforementioned Form must be completed and submitted to CySEC within fifteen (15) days from the end of each month.

According to Circular CI144-2013-17, the scanned copy of the duly completed and signed Form 144-08-11 should be submitted to CySEC only electronically at the electronic address:

EVERYTHING YOU NEED AND MORE

mviolari@cysec.gov.cy. The subject of the said email should include the name of the Obligated Entity as well as the reporting month to which the form it relates. The original completed and signed form must be kept in the Obligated Entity's offices.

The completion of the aforementioned Form provides the opportunity to the Obligated Entity 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 is responsible to review, at least annually as per Section 3.1 of the Manual, the submission to CySEC of the "Monthly prevention statement regarding the prevention of Money Laundering and Terrorist Financing".

7. Risk Based Approach

7.1 Approach Outline

The Obligated Entity shall apply appropriate measures and procedures, by adopting a risk-based approach, based on the Risk-Based Supervision Guidelines issued by the ESAs in accordance with Article 48 (10) of Directive (EU) 2015/849, 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 MLCO 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 Obligated Entity, and described in the Manual, has the following general characteristics:

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

The Obligated Entity takes also into account the risk factors stated in the ESA Guidelines, including the sectoral guidelines for investment firms.

There are three type of risk factors, the product, service or transaction risk factors, the customer risk factors and the Country or geographical risk factors.

Product, service or transaction risk factors

The following factors may contribute to increasing risk:

- transactions are unusually large;
- third party payments are possible;
- the product or service is used for subscriptions that are quickly followed by redemption possibilities, with limited intervention by the investment manager.

Customer risk factors

The following factors may contribute to increasing risk:

- The customer's behaviour, for example:
- the rationale for the investment lacks an obvious economic purpose;
- the customer asks to repurchase or redeem a long-term investment within a short period after the initial investment or before the payout date without a clear rationale, in particular where



EVERYTHING YOU NEED AND MORE

this results in financial loss or payment of high transaction fees;

- the customer requests the repeated purchase and sale of shares within a short period of time without an obvious strategy or economic rationale;
- unwillingness to provide CDD information on the customer and the beneficial owner;
- frequent changes to CDD information or payment details;
- the customer transfers funds in excess of those required for the investment and asks for surplus amounts to be reimbursed;
- the circumstances in which the customer makes use of the ‘cooling-off’ period give rise to suspicion;
- using multiple accounts without previous notification, especially when these accounts are held in multiple or high-risk jurisdictions;
- the customer wishes to structure the relationship in such a way that multiple parties, for example nominee companies, are used in different jurisdictions, particularly where these jurisdictions are associated with higher ML/TF risk.

The customer’s nature, for example:

- the customer is a Obligated Entity or trust established in a jurisdiction associated with higher ML/TF risk (firms should pay particular attention to those jurisdictions that do not comply effectively with international tax transparency standards);
- the customer is an investment vehicle that carries out little or no due diligence on its own clients;
- the customer is an unregulated third-party investment vehicle;
- the customer’s ownership and control structure is opaque;
- the customer or the beneficial owner is a PEP or holds another prominent position that might enable them to abuse their position for private gain;
- the customer is a non-regulated nominee Obligated Entity with unknown shareholders.

The customer’s business, for example the customer’s funds are derived from business in sectors that are associated with a high risk of financial crime.

Country or geographical risk factors

The following factors may contribute to increasing risk:

- The investor or their custodian is based in a jurisdiction associated with higher ML/TF risk.
- The funds come from a jurisdiction associated with higher ML/TF risk

7.2 Measures & Procedures

The risk-based approach adopted by the Obligated Entity, 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 Obligated Entity.

Such measures include:

1. identifying and assessing the Money Laundering and Terrorist Financing risks emanating from particular Clients or types of Clients, financial instruments, services, and geographical



EVERYTHING YOU NEED AND MORE

areas of operation of its Clients;

2. managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls; and

3. 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:

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

The MLCO shall be responsible for the development of the policies, procedures and controls on a risk-based approach. Further, the MLCO 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 MLCO, at least annually, as per Section 3 of the Manual.

7.3 Identification of Risks

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

The Obligated Entity 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 Obligated Entity 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 Obligated Entity provides are relatively simple, involving relatively few Clients or Clients with similar characteristics, then the Obligated Entity shall apply such procedures which are able to focus on those Clients who fall outside the 'norm'.

The Obligated Entity 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.

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

- (a) Risks based on the Client's nature:
- complexity of ownership structure of legal persons;
 - companies with bearer shares;
 - companies incorporated in offshore centers;
 - PEPs;
 - Clients engaged in transactions which involve significant amounts of cash;
 - Clients from high risk countries or countries known for high level of corruption or organised crime or drug trafficking; and
 - unwillingness of Client to provide information on the Beneficial Owners of a legal person.
- (b) Risks based on the Client's behaviour:
- Client transactions where there is no apparent legal financial/commercial rationale;
 - situations where the origin of wealth and/or source of funds cannot be easily verified; and
 - unwillingness of Clients to provide information on the Beneficial Owners of a legal person.
- (c) Risks based on the Client's initial communication with the Obligated Entity:
- non face-to-face Clients; and
 - Clients introduced by a third person.
- (d) Risks based on the Obligated Entity's services and financial instruments:
- services that allow payments to third persons/parties;
 - large cash deposits or withdrawals; and
 - products or transactions which may favour anonymity.

7.4 Design and Implementation of Measures and Procedures to Manage and Mitigate Risks

Taking into consideration the assessed risks, the Obligated Entity 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:

- a) adaption of the CDD Procedures in respect of Clients in line with their assessed Money Laundering and Terrorist Financing risk;
- b) 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);
- c) 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; and
- d) on-going monitoring of high risk Clients' transactions and activities, as and when applicable.

In this respect, it is the duty of the MLCO to develop and constantly monitor and adjust the Obligated Entity's policies and procedures with respect to the Client Acceptance Policy and CDD 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.

7.5 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 Obligated Entity 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 MLCO 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.

7.6 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 MLCO and the Administration/Back-Office Department shall consult data, information and reports [e.g. Clients from countries which inadequately apply 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; and
- f) The International Monetary Fund (IMF) – www.imf.org.

8. Client Acceptance Policy

8.0 General Principles of the CAP

The General Principles of the CAP are the following:

- a) the Obligated Entity 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 9 of the Manual;
- c) all documents and data described in Section 9.6 of the Manual must be collected before accepting a new Client;
- d) no account shall be opened in anonymous or fictitious names(s); and
- e) no account shall be opened unless the prospective Client is approved by the MLCO.

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

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

8.1.1 Low Risk Clients

The Obligated Entity shall accept Clients who are categorised as low risk Clients as long as the general principles under Section 8.0 are followed.

Moreover, the Obligated Entity shall follow the Simplified Client Identification and Due Diligence Procedures for low risk Clients, according to Section 9.9 of the Manual.

8.1.2 Normal Risk Clients

The Obligated Entity shall accept Clients who are categorised as normal risk Clients as long as the general principles under Section 8.0 of the Manual are followed.

8.1.3 High Risk Clients

The Obligated Entity shall accept Clients who are categorised as high risk Clients as long as the general principles under Section 8.0 of the Manual are followed.

Moreover, the Obligated Entity shall apply the Enhanced Client Identification and Due Diligence measures for high risk Clients, according to Section 9.9 of the Manual and the due diligence and identification procedures for the specific types of high risk Clients mentioned as well in Section 8.2.3 of the Manual, as applicable.

8.1.4 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 Obligated Entity:



EVERYTHING YOU NEED AND MORE

- a) Clients who fail or refuse to submit, the requisite data and information for the verification of their identity and the creation of their economic profile (appropriateness test), without adequate justification (see also Section 9.4 of the Manual);
- b) Shell Banks; and
- c) Credit institutions, obliged entities 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 an operating license for providing services from CySEC or any other relevant regulatory authority of the Republic of Cyprus, in view of Circular CI144-2008-11.
- d) Clients who have been convicted/accused for wrongdoings including but not limited to Money Laundering, Criminal activities etc.
- e) Clients from Banned Jurisdictions (Please see Appendix IV)

Only clients who have passed the Obligated Entity's Appropriateness test shall be accepted.

Clients who did not pass the appropriateness test, shall be accepted only if such clients acknowledged the relevant risk warning, in which case clients may proceed with the establishment of the business relationship at their own risk.

8.2 Client Categorisation Criteria

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

8.2.1 Low Risk Clients

The following types of Clients can be classified as **low risk Clients** with respect to the Money Laundering and Terrorist Financing risk which the Obligated Entity faces and there is no suspicion for money laundering or terrorist financing:

- (a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
- (b) public administrations or enterprises;
- (c) customers that are resident in geographical areas of lower risk as set out in point (3);
- (d) credit or financial institution covered by the EU Directive;
- (e) credit or financial institution carrying out one or more of the financial business activities as these are defined by the Law and which is situated in a country outside the EEA, which:
 - i. in accordance with a decision of the Advisory Authority, imposes requirements equivalent to those laid down by the EU Directive (see Appendix IV for the list of equivalent third countries), and
 - ii. it is under supervision for compliance with those requirements;
- (f) listed companies whose securities are admitted to trading on a Regulated Market in a country of the EEA or in a third country which is subject to disclosure requirements consistent with community legislation; and domestic public authorities of countries of the EEA.



EVERYTHING YOU NEED AND MORE

- (g) life insurance policies for which the premium is low;
- (h) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
- (i) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;
- (j) 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;
- (k) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money);
- (l) Member States;
- (m) third countries having effective AML/CFT systems;
- (n) third countries identified by credible sources as having a low level of corruption or other criminal activity;
- (o) 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.

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

It is provided further that the Obligated Entity is obliged to exercise continuous monitoring of the business relationships mentioned in paragraphs (a) to (o) of this section according to the provisions of the paragraph (d) of section 1 of article 61 of the Law and report to the Unit circumstances of conducting or attempted conducting of suspicious transactions.

It is provided that further to the cases mentioned above, the Obligated Entity has to gather sufficient information to establish if the Client qualifies as a low-risk Client. In this respect, the MLCO 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 12.

- **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 Obligated Entity faces:

- any Client who does not fall under the 'low risk Clients' or 'high risk Clients' categories set in Sections 8.2.1 and 8.2.3, respectively.

- **High Risk Clients**

The following types of Clients can be classified as high-risk Clients with respect to the Money Laundering and Terrorist Financing risk which the Obligated Entity faces:

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

- Clients whose own shares or those of their parent companies (if any) have been issued in bearer form;
- trust accounts;
- ‘Client accounts’ in the name of a third person;
- PEPs’ accounts;
- Clients who are involved in electronic gambling/gaming activities through the internet;
- Clients from countries which inadequately apply FATF’s recommendations;
- cross-frontier correspondent banking relationships with credit institutions-Clients from third countries; (products or transactions that might favour anonymity;)
- any other Clients that their nature entail a higher risk of money laundering or terrorist financing; and
- any other Client determined by the Obligated Entity itself to be classified as such.
- customers that are resident in geographical areas of higher risk as set out below
- legal persons or arrangements that are personal asset-holding vehicles;
- businesses that are cash-intensive;
- the ownership structure of the Obligated Entity appears unusual or excessively complex given the nature of the Obligated Entity’s business;
- private banking;
- non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;
- payment received from unknown or unassociated third parties;
- 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
- countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
- countries identified by credible sources as having significant levels of corruption or other criminal activity;
- countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;
- countries providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

9. Client Due Diligence & Identification Procedures

9.1 Application of Procedures

The Obligated Entity shall duly apply Client identification procedures and CDD measures in the



EVERYTHING YOU NEED AND MORE

following cases:

- a) when establishing a Business Relationship;
- b) when carrying out Occasional Transactions amounting to €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;
- d) when there are doubts about the veracity or adequacy of previously Client identification data
- e) To all new and clients but also existing clients at appropriate times, depending on the level or risk of being involved in money laundering or terrorist financing.

In this respect, it is the duty of the MLCO to apply all the relevant CDD Identification Procedures described in the Manual for the five (5) cases mentioned above. Furthermore, the Back-Office Department shall also be responsible to collect and file the relevant Client identification documents, according to the recording keeping procedures described in Section 12 of the Manual.

The Head of the Back- Office Department shall be a qualified and experienced person and shall be responsible for the creation, managing, and monitoring of the clients' accounts. Moreover, the Head of the Department shall report to the Senior Management of the Obligated Entity who shall be responsible for the supervision of the Department.

In particular, the Back Office/ Account opening department in collaboration with the Customer Support department where appropriate, will be responsible for the following functions:

- Open a new client account
- Maintenance of a client account
- Funds Transfer
- Deposit of incoming funds
- Withdrawal of outgoing funds
- Marketing communication

The procedures which are followed by the Head of the Back-Office Department in relation to the performance of the duties are the following:

9.2 Open a new client account

The Department shall be responsible to ensure that all information required for the opening of an account for client are collected and are properly reviewed. The procedure followed in collecting the information is described below. The requirements of the documents to be collected are in accordance with Anti-Money Laundering and Know Your Client Policy of the Obligated Entity. In this respect, the head of the department should be regularly updated for the requirements of the relevant legislation and when needed implements necessary



EVERYTHING YOU NEED AND MORE

changes to the procedures and forwards these to the Senior Management for approval. Opening of the account to new Client is approved by the Obligated Entity's AMLCO by signing letter of notification.

9.3 Physical persons accounts

Client identification process performed prior to opening new accounts:

Prior to accepting new clients and allowing them to trade with the Obligated Entity, the following documents shall be obtained:

9.2.1 Proof of Identity:

1. A certified true copy of the client's passport or ID card (only for residents of the Republic of Cyprus). Copy of the original documents/data obtained are accepted provided that at least one of the conditions mentioned under sub-paragraph (a) is followed:
 - (a) In addition to the measure under section 64(1)(a)(ii) of the Law 188(I)/2007, practical procedures that can be applied as implementing measures of section 64(1)(a)(i) and (ii) of the Law 188(I)/2007 regarding non-face to face customers of the Obligated Entity are the following:
 - i. Ensure that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution which operates in a country within the European Economic Area or in a third country that the Advisory Authority for Combating Money Laundering and Terrorist Financing has determined to be applying procedures and measures for the prevention of money laundering and terrorist financing equivalent to the European Union Directive.
 - ii. Obtain direct confirmation for the establishment of a business relationship via the direct personal contact, regarding the prospective customer's true name, address and passport / identity card number (only for residents of the Republic of Cyprus) from a credit institution or financial institutions that the client collaborates with, that operates in a Member State or in a third country that the Advisory Authority for Combating Money Laundering and Terrorist Financing has determined to be applying procedures and measures for the prevention of money laundering and terrorist financing equivalent to the European Union Directive (or a certified true copy of the confirmation).
 - iii. Contact the customers via telephone at their residence or office, before the establishment of a business relationship or the occasional transaction, on a

telephone number which has been verified from a reliable and independent source. During the telephone correspondence, the Obligated Entity shall verify other information submitted by the customers during the account opening procedure.

- iv. Contact the customers via call, provided that the safeguards of the call are recorded and evidence of the conversation is ensured. It is provided that in case where the verification of the customers / beneficial owners' identity has not been completed based on the provisions of the respective paragraph, the cumulative amount of deposited funds of customers / beneficial owners should not exceed €2,000, irrespective of the number of accounts the customers / beneficial owners hold with the Obligated Entity, in case where no additional measures of this section or of the article 64(1)(a)(ii) of the Law 188(I)/2007, have been taken.

It is provided that the Obligated Entity is required to implement appropriate measures and procedures in order to:

1. Verify and monitor the amount deposited by the customer as well as the risk of money laundering and terrorist financing or terrorist financing operations and applies enhanced measures for the verification of customer's identity, depending on the degree of risk.
 2. Ensure the normal conduct of business in case where the cumulative amount of deposited funds of customers /beneficial owners has not exceeded €2,000.
 3. Warn its customers appropriately and sufficiently in due time regarding the above procedure and receive their explicit consent as to the procedure that is to be followed, before the establishment of the business relationship.
- v. Contact the customer via email at an email address which has been verified from a reliable and independent source, through registered mail (for example, the correspondence may include documents required for the account opening, which the customers must return to the Obligated Entity or a password that the customers require to access their online account).

vi. Verify the customers' identity via electronic means:

1. The verification of the customers' identity via electronic means is performed by the Obligated Entity or by a third person. All the following

EVERYTHING YOU NEED AND MORE

- conditions, cumulatively are satisfied by the Obligated Entity and the third person:
- i. The online databases that the third person or the Obligated Entity has access, is registered in, and / or approved by the Commissioner for the Protection of Personal Data for the purpose of maintaining personal data (or the competent authority in the country that the database is maintained).
 - ii. The online databases provide access to information regarding both current and past statements indicating that indeed the person existed and contains both positive information (as a minimum the full name, address and the customers' date of birth) and negative information (e.g. committing crimes like identity theft, included in deceased persons lists, included in sanctions lists and restrictive measures issued by the Council of the European Union and the UN Security Council).
 - iii. The electronic databases contain a wide range of sources with information from various time intervals, which are updated in real time and trigger alerts when important data are differentiate.
 - iv. Transparent procedures have been implemented, which enable the Obligated Entity to know what information has been investigated, what are the results and their significance in relation to the degree of certainty with respect to the verification of the customer.
 - v. Procedures have been established that enable the Obligated Entity to record and maintain information used and the results in regards to the verification of customers' identity.
2. The Obligated Entity evaluates the results of the verification of customers' identity via electronic means in order to ensure that the provisions of article 61(3) of the Law 188(I)/2007 are satisfied. The Obligated Entity establishes mechanisms for the implementation of quality controls in order to assess the quality of information that the Obligated Entity intends to rely on.
 3. The information should be derived from two or more sources. As a minimum, the verification procedure via electronic means shall meet the following correlation model:
 - i. identification of the customers' full name and current address using the same source, and
 - ii. identification of the customers' full name and either their current address or date of birth using a different source.



EVERYTHING YOU NEED AND MORE

4. For the purposes of the verification of customers' identity via electronic means, the Obligated Entity must establish procedures so as to ensure the completeness, accuracy and reliability of the information obtained. It is provided that the results of the verification process should include both positive and negative information.

9.2.2 Proof of Address:

A utility bill, house deed or bank statement not older than 6 months, stating the client's name and residential address. In cases where the clients are operating within countries where the addresses are identified only by reference to a P.O. Box, a declaration letter signed by an independent government representative or professional officer (such as post office, lawyer, accountants and notary public) confirming the client's address is accepted. Moreover, in cases where the clients are living with a family member and the only proof of address they can produce is in the name of the relative, a declaration confirming the family relationship is accepted to verify the validity of the proof of address provided.

In addition, personal details of the client are verified through information provided by the payment service provider (e.g. bank, credit card Obligated Entity) to ensure that they are identical to the information provided by the client during the application process.

If the clients fail to provide the requested documentation, the clients' accounts will not be activated in order to be able to start trading until the KYC procedures are satisfactory completed. Should the client wish to close his/her account or refuse to provide the necessary documents, the client will be allowed to withdraw his/her funds within 5 working days upon his/her request.

Should the Obligated Entity not be able to complete the customer's verification process the following shall occur:

- If the Obligated Entity considers the account to fall under the "suspicious transaction" definition, the Obligated Entity will submit a suspicious transaction report to the Unit for Combating Money Laundering (MOKAS).
- If the Obligated Entity does not consider the account to fall under the "suspicious transaction" definition, the Obligated Entity will suspend the account and if the customer fails to comply with the Obligated Entity's requirements, the Obligated Entity shall close permanently the account.

9.2.3 Legal persons accounts

A different identification procedure is followed for legal persons interested in opening an account with the Obligated Entity. The documentation that needs to be obtained by the corporate client is presented below:

a) Verification of the natural person which is acting on behalf of the legal entity



EVERYTHING YOU NEED AND MORE

- Board resolution authorizing the person to act on behalf of the Obligated Entity
 - Copy of the passport and utility bill of that person.
- b) Full ascertainment of the legal entity's control and ownership structure and verification of the identity of the beneficial owners and those exercise control over the legal entity**
- If a regulated entity, copy of the license and copy of directors' certificate
 - If not regulated entity, legal structure (if part of a group of companies) and KYC documents for all beneficial owners holding above 10% of the share capital
- c) Verification of the identity of the legal entity**
- Certificate of incorporation and certificate of good standing
 - Certificate of registered office
 - Certificate of directors and secretary
 - Certificate of shareholders
 - Certificate of Incumbency, if applicable (shall replace certificates of incorporation, registered office, directors and secretary and shareholders)
 - Memorandum and articles of association (if not EU regulated or regulated in a country with equivalent disclosure and transparency requirements)
 - In case that registered shareholders act as nominees of the beneficial owners, a copy of the trust agreement concluded between the nominee shareholder and the beneficial owners
 - Documents for the verification of the identity of the registered shareholders and the beneficial owners (passport and utility bill)
 - Legal Person's LEI number

In accordance with the legislation the above documents shall be obtained in their original form or as certified true copies of the original.

9.2.4 Accounts maintenance

Back Office / Account Opening Department shall be responsible for carrying out the following accounts maintenance activities:

a) Archiving

All archived records must be kept for a minimum of 5 years. Documentation kept electronically will remain in the system until the client has ceased to have a relationship with the Obligated Entity. When this occurs, the documentation will then be stored in the archiving system as history information.

b) Monitoring

All clients' accounts shall be closely monitored by the Obligated Entity's Back Office Department. The Obligated Entity's CRM has been updated in regards to its functionalities,

EVERYTHING YOU NEED AND MORE

therefore, where a client's KYC document is almost expired,

- the CRM notifies the Back-Office Department (with red flags), one month prior the document's expiration.
- The Back Office then notifies the client via email in regards to the expiration of the document 4 weeks prior the expiration of his documents and requests an updated document.
- The Back Office then sends additional email in regards to the expiration of the document and informs the client of the downfalls should he fails to update his documents. This happens two weeks after he initial notification email.
- The Back Office then contacts the client via telephone in order to inform the client in regards to the expiration of his documents. This happens 3 days before the expiration of his documents.
- From the date of the expiration of the document, the client is given 5 days to send the updated document.
- In case where the client fails to send the updated document as requested, the Back-Office Department shall change the access to read only its account. No transactions shall be accepted. Reactivation of account shall only be made upon receipt of a new valid document.

c) Deletion of an account

The removal of an account from the system shall be the sole responsibility of Back Office / Account Opening Department which will obtain an approval by Senior Management.

d) Closing of a client's account

Back Office / Account Opening Department shall be responsible for closing a client's account under the following circumstances:

- ***Closing of an account upon client's request***

If a client requests to close his/her account, Back Office / Account Opening Department must verify that the client provides them with clear instructions about their request in written form. In turn, funds in client's accounts shall all be withdrawn and settled within 5 working days. Note that Back Office Department must keep all records and transactions made by the client for at least 5 years after the termination of his/her account.

- ***Closing of an account when client has passed away***

If a client has passed away, the inheritor or the person who acts on behalf of the client (e.g. lawyer) is responsible for providing instructions to the Back Office Department for closing the client's account. The Back-Office Department shall also request a Death's Certificate, as well as the bank details of the inheritor(s) for transferring the underlying funds to the inheritor.

Further, the MLCO shall be responsible to maintain at all times and use during the

application of CDD and identification procedures template-checklists with respect to required documents and data from potential Clients, as per the requirements of the Law and the Directive.

The Internal Auditor shall be responsible to review the adequate implementation of all the policies and procedures mentioned in Section 3 of the Manual, at least annually.

9.3 Ways of application of Client Identification and Due Diligence Procedures

Client identification procedures and CDD measures shall comprise:

- 9.3.1 identifying the Client and verifying the Client's identity on the basis of documents, data or information obtained from a reliable and independent source;
- 9.3.2 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;
- 9.3.3 obtaining information on the purpose and intended nature of the business relationship;
- 9.3.4 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.

9.4 Transactions that Favor 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 Obligated Entity 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.

EVERYTHING YOU NEED AND MORE

9.5 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 9.6 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 Obligated Entity shall not proceed with the establishment of the Business Relationship or the execution of the occasional transaction (see Section 8.1.4 of the Manual) while at the same time the MLCO considers whether it is justified under the circumstances to submit a report to the Unit, according to point (g) of Section 4.2 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 Obligated Entity and the MLCO shall consider terminating the Business Relationship and close all the accounts of the Client, taking also into account the specific circumstances of the Client in question and the risks faced by the Obligated Entity 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 4.2 of the Manual.

It should be noted, that the Obligated Entity relies on the provisions of article 62(2) of the AML Law which the cumulative amount of the funds deposited by a client should not exceed EURO 2,000 and the cumulative time in which the verification of the clients' identity is completed must not exceed 15 days from the date the account was opened. In case where the client does not comply with the above requirement, all the accounts of the Client shall be terminated.

9.6 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 MLCO 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 Client 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. In such situations, these procedures shall be completed as soon as possible after the initial contact and before any transactions are conducted.
3. In cases where the Obligated Entity is unable to comply with points 1(a) to 1(h) of

Section

EVERYTHING YOU NEED AND MORE

9.7 of the Manual, the Obligated Entity shall not carry out any transaction through a bank account, establish a Business Relationship or carry out an Occasional Transaction and consider making a report to the Unit; and

4. Identification procedures and CDD requirements shall be applied not only to all new Clients but also to existing Clients at appropriate times, depending on the level of risk of being involved in money laundering or terrorist financing (Section 8.2 of the Manual).

9.7 Construction of Economic Profile, Client Identification & Due Diligence Principles

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

- a) the Obligated Entity shall be satisfied that it's dealing with a real person and, for this reason, the Obligated Entity shall obtain sufficient evidence of identity to verify that the person is who he claims to be. Furthermore, the Obligated Entity shall verify the identity of the Beneficial Owner(s) of the Clients' accounts. In the cases of legal persons, the Obligated Entity 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 Obligated Entity 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;
- 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 Obligated Entity will never use the same verification data or information for verifying the Client's identity and verifying his/her 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:
 - i. the purpose and the reason for requesting the establishment of a Business Relationship;
 - ii. the anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments; and
 - iii. the Client's size of wealth and annual income and the clear description of the main business/professional activities/operations
- f) the data and information that are used for the construction of the Client-legal person's economic profile shall include, inter alia, the following:
 - i. the name of the Obligated Entity;
 - ii. the country of its incorporation;

EVERYTHING YOU NEED AND MORE

- iii. the head offices address;
 - iv. the names and the identification information of the Beneficial Owners;
 - v. the names and the identification information of the directors;
 - vi. the names and the identification information of the authorised signatories;
 - vii. financial information; and
 - viii. the ownership structure of the group that the Client-legal person may be a part of (country of incorporation of the parent Obligated Entity, subsidiary companies and associate companies, main activities and financial information).
- g) 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.
- h) 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; and
- i) 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 MLCO, according to point (e) of Section 4.2 of the Manual, and then by the latter to the Unit, according to point (g) of Section 4.2 of the Manual.

2. The Obligated Entity shall apply each of the CDD 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 Obligated Entity shall be able to demonstrate to CySEC that the extents of the measures are 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 CDD 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 MLCO. 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

9.8 Further Obligations for Client Identification and Due Diligence Procedures

1. In addition to the principles described in Section 9.6 above, the Obligated Entity, and specifically the MLCO 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.
- c) The procedures and controls of point (a) in Section 4.2 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 Obligated Entity becomes aware that reliable or adequate data and information are missing from the identity and the economic profile of the Client, then the Obligated Entity 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 Obligated Entity 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:
 - a. change of directors/secretary;
 - b. change of registered shareholders and/or Beneficial Owners;
 - c. change of registered office;
 - d. change of trustees;
 - e. change of corporate name and/or trading name; and
 - f. change of the principal trading partners and/or undertaking of major new business activities.
- c) a material change in the way and the rules the Client's account operates, such as:
 - a. change in the persons that are authorised to operate the account; and
 - b. application for the opening of a new account for the provision of new investment services and/or financial instruments.

4. In addition to the above, the Obligated Entity, when making transfers of money between Clients' accounts, shall apply the following procedures in accordance to Circular CI144-2012-09, as applicable:

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

9.9 Simplified Client Identification and Due Diligence Procedures

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

- 9.9.1 In the cases of points (a), (b) (c) and (d) of Section 9.1, the Obligated Entity may not apply the measures described in Section 9.2, point (1) of Section 9.5 and Sections 9.6 and 9.7 of the Manual for a Client who may be categorized as a low risk Client according to the criteria set in Section 8.2.1 of the Manual, provided the Obligated Entity performs continuous monitoring of the client's trading account to ensure there is no suspicious trading nor changes in the client's normal course of activity.
- Furthermore, where the Client is categorized as a low risk Client (according to the criteria set in Section 8.2.1 of the Manual) the verification of the identity of the Client and the Beneficial Owner may be completed during the establishment of a Business Relationship if this is necessary not to interrupt the normal conduct of business and where the risk of money laundering or terrorist financing occurring is low. In such situations, these procedures shall be completed as soon as possible after the initial contact and before any transactions are conducted.
- 9.9.2 It is provided that the Obligated Entity 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 8.2.1. The Obligated Entity 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



EVERYTHING YOU NEED AND MORE

laundering or terrorist financing purposes.

9.9.3 The Obligated Entity 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

9.9.4 With respect to public authorities or public bodies of the EEA countries, for which the provisions of point (1) of Section 9.6 may not be applied, they must fulfil all the following criteria:

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

9.9.4.2 the Client's identity is publicly available, transparent and certain;

9.9.4.3 the activities of the Client, as well as its accounting practices, are transparent; and

9.9.4.4 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.

9.10 Enhanced Client Identification and Due Diligence (High Risk Clients)

The MLCO shall apply enhanced due diligence measures, in addition to the measures referred to in Sections 9.2, 9.5, 9.6 and 9.7, with respect to the Clients categorized as high-risk Clients according to the criteria set in Section 8.2.3 of this Manual.

These measures include the following:

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

- i. take supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution; and
- ii. 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.

(b) In respect of cross-frontier correspondent banking relationships with credit institutions-Clients from third countries, the Obligated Entity 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 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;

EVERYTHING YOU NEED AND MORE

- v. document the respective responsibilities of the person engaged in financial or Other Business Activities and of the credit institution-Client; and
 - vi. with respect to payable-through accounts, must be ensured that the credit institution-Client has verified the identity of its Clients and performed ongoing 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 Obligated Entity shall:
- i. have appropriate risk-based procedures to determine whether the Client (or the Beneficial Owner) is a PEP;
 - ii. have Senior Management approval for establishing Business Relationships with such Clients or for the continuation of the business relationships with existing Clients which have become PEPs;
 - iii. take adequate measures to establish the source of wealth and source of funds; and
 - iv. conduct enhanced on-going monitoring of the Business Relationship. Provided the client is no longer considered to be a PEP in the Republic of Cyprus, nor in any other EU Member State nor in a third world country and does not hold a key position in an international organization. The Obligated Entity should take into consideration all of the above, along with the risk the particular client might still pose to the Obligated Entity even after his termination of his PEP duties, and takes the necessary steps to mitigate such risk for at least the next 12 (twelve) consecutive months from the client's termination of his PEP duties, until he no longer poses danger/threat.
 - v. The Obligated Entity shall apply the same measures mentioned in points (i) and (ii) to the Client's close relatives or persons whom are known to be closely related or collaborators of the PEP.

Below are described due diligence and identification procedures with respect to high risk Clients:

9.11 Non-face-to-face Clients

The MLCO shall apply the following with respect to non-face-to-face Clients:

- 9.11.1 In situations where a Client, especially a non-resident of the Republic, requests the establishment of a Business Relationship or an Occasional Transaction through mail, telephone, or the internet without presenting himself for a personal interview, the Obligated Entity must follow the established Client identification and due diligence procedures, as applied for Clients with whom it comes in direct and personal contact and obtain exactly the same identification information and documents.

However, due to the difficulty in matching the Client with the collected identification data, the

Obligated Entity shall apply enhanced Client identification and due diligence measures, in line with the provisions of Section 9.9. of the Manual, so as to effectively mitigate the risks associated with such Business Relationship or Occasional Transaction.

9.11.2 Practical procedures that can be applied as implementation of the measures of points (a)(i) of Section 9.9 regarding non-face-to-face Clients of the Obligated Entity are the following:

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

9.11.2.2 obtaining a reference letter from a third person, according to Section 9.13;

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

9.11.2.4 contact with the Client through mail at an address previously verified by the Obligated Entity from independent and reliable sources.

9.11.3 The provisions of point (a) of Section 9.9. are also applied to companies or other legal persons requesting the establishment of a Business Relationship or an Occasional Transaction through mail, telephone or internet. The Obligated Entity shall take additional measures for ensuring that the companies or other legal persons operate from the address of their main offices and carry out legitimate business activities.

9.12 Account in names of companies whose shares are in bearer form

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

The Obligated Entity 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 9.9, all the following supplementary due diligence measures:

- a. the Obligated Entity 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 Obligated Entity 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 9.26, 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 Obligated Entity-Client or that of its holding Obligated Entity (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 Obligated Entity-Client, then the written confirmation is provided by the Obligated Entity-Client's directors; and
- d. when there is a change to the Beneficial Owners, the Obligated Entity examines **whether or not to permit the continuance of the account's operation.**

9.13 Trust accounts

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

- 9.13.1 When the Obligated Entity 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 Section 11 of this Manual.
- 9.13.2 Furthermore, the Obligated Entity 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.

9.14 'Client accounts' in the name of a third person

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

- 9.14.1 The Obligated Entity 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 applies procedures and measures for preventing Money Laundering and Terrorist Financing equivalent to the requirements of the EU Directive (see Appendix IV for the list of equivalent third countries). In these cases, the Obligated Entity shall ascertain the identity of the abovementioned financial institutions according to the Client identification procedures prescribed in throughout Section 9 of the Manual.

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

institution and any additional measures deemed necessary during the assessment. It is stressed that the Obligated Entity shall be extra vigilant on such cases.

- 9.14.2 In the case that the opening of a “client account” is requested by a third person acting as an auditor/accountant or an independent legal professional or a trust and Obligated Entity service provider situated in 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 and measures for preventing money laundering and terrorist financing equivalent to the requirements of the EU Directive (see Appendix IV for the list of equivalent third countries), the Obligated Entity shall proceed with the opening of the account provided that the following conditions are met:
- 9.14.2.1 the third person is subject to mandatory professional registration in accordance with the relevant laws of the country of operation;
 - 9.14.2.2 the third person is subject to regulation and supervision by an appropriate competent authority in the country of operation for Anti-Money Laundering and Terrorist Financing purposes;
 - 9.14.2.3 the MLCO has assessed the Client identification and due diligence procedures implemented by the third person and has found them to be in line with the Law and the Directive. A record of the assessment should be prepared and kept in a separate file maintained for each third person; and
 - 9.14.2.4 the third person makes available to the Obligated Entity all the data and documents prescribed in point (1) of Section 9.13 of the Manual.

9.15 “Politically Exposed Persons” accounts

The Obligated Entity shall apply the following with respect to the accounts of “Politically Exposed Persons”:

- 9.15.1 The establishment of a Business Relationship or the execution of an Occasional Transaction with persons holding important public positions in Cyprus or abroad and with natural persons closely related to them, may expose the Obligated Entity 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 Obligated Entity 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.

- 9.15.2 In order to effectively manage such risks, the Obligated Entity 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+9 requirements of the FATF,

according to Section 9.16 of the Manual.

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+9 recommendations of the FATF, the Obligated Entity 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.

- 9.15.3 According to the general definition, PEPs are the natural persons who are residing in Cyprus or abroad and who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons.
- 9.15.4 The meaning 'Politically Exposed Persons' includes the following natural persons who are or have been entrusted with prominent public functions' in Cyprus or abroad:
- 9.15.4.1 heads of State, heads of government, ministers and deputy or assistant ministers;
- 9.15.4.2 members of parliaments;
- 9.15.4.3 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;
- 9.15.4.4 members of courts of auditors or of the boards of central banks;
- 9.15.4.5 ambassadors, charges des affaires and high-ranking officers in the armed forces; and
- 9.15.4.6 members of the administrative, management or supervisory bodies of State- owned enterprises.
- 9.15.5 Without prejudice to the application, on a risk-sensitive basis, of enhanced CDD measures (Section 9.9 of the Manual), where a person has ceased to be entrusted with a prominent public function within the meaning of point (4) above for a period of at least one year, the Obligated Entity shall not be obliged to consider such a person as politically exposed.
- 9.15.6 None of the categories set out in point (4) above shall be understood as covering middle ranking or more junior officials. 'Immediate family members' includes the following:
- (a) the spouse or the person with which cohabit for at least one year;
 - (b) the children and their spouses or the persons with which cohabit for at least one year; and
 - (c) the parents.
- 9.15.7 'Persons known to be close associates' includes the following:
- (a) any natural person who is known to have joint Beneficial Ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in point (4) above;

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

9.15.8 Without prejudice to the provisions of point (c) Section 9.9 of the Manual, the Obligated Entity adopts the following additional due diligence measures when it establishes a Business Relationship or carry out an Occasional Transaction with a PEP:

- (a) the Obligated Entity 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 an Executive Director of the Obligated Entity and the decision is then forwarded to the MLCO. 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 an Executive Director of the Obligated Entity which is then forwarded to the MLCO;
- (c) before establishing a Business Relationship or executing an Occasional Transaction with a PEP, the Obligated Entity 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 Obligated Entity shall create the economic profile of the Client by obtaining the information specified in Section 9.6. The details of the expected business and nature of activities of the Client forms the basis for the future monitoring of the account. The profile shall be regularly reviewed and updated with new data and information. The Obligated Entity shall be particularly cautious and most vigilant where its Clients are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks; and
- (e) the account shall be subject to annual review in order to determine whether to allow its continuance of operation. A short report shall be prepared summarizing the results of the review by the person who is in charge of monitoring the account. The report shall be submitted for consideration and approval to the Board and filed in the Client's personal file.

9.16 Electronic gambling & gaming through the internet

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

- 9.16.1 The Obligated Entity 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 (see Appendix IV for the list of equivalent third countries). For this purpose, the Obligated Entity shall request and obtain, apart from the data and information required by the Manual, copy of the license that has been granted to the said persons by the competent supervisory/regulatory authority, the authenticity of which must be verified either directly with the supervisory/regulatory authority or from other independent and reliable sources.
- 9.16.2 Furthermore, the Obligated Entity shall collect adequate information so as to understand the Clients' control structure and ensure that the said Clients apply adequate and appropriate systems and procedures for Client identification and due diligence for the prevention of money laundering and terrorist financing.
- 9.16.3 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 Obligated Entity 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 Obligated Entity shall obtain the signed agreement between its Client and the Obligated Entity that is duly licensed for electronic gambling/gaming activities through the internet, by a competent authority of a country mentioned in point (1) above.
- 9.16.4 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 Obligated Entity and the decision is then forwarded to the MLCO. 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

9.17 Clients from high risk third countries

9.17.1 According to the Prevention and Suppression of Money Laundering and Terrorist Financing Laws of 2007-2018, “high risk third countries” are the countries that present strategical shortcomings in their national system for combating money laundering and terrorist financing.

9.17.2 It includes the third countries that are:

- Are considered as important threats for the financial system of the European Union and are declared in the issued acts by way of derogation and
- Are categorized by the obliged entities as high risk in accordance with the risk assessment foreseen by Article 58A of the Law.

9.17.3 The Obligated Entity according to the Prevention and Suppression of Money Laundering and Terrorist Financing Laws of 2007-2018, shall apply enhanced customer due diligence measures, in addition to the measures referred to below and in other cases which by their nature, present a high risk of money laundering or terrorist financing

Provided that when assessing the said risks, the Obligated Entity takes into account the factors of potentially higher risk situations, as set out below:

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) customers that are resident in geographical areas of higher risk as set out in Annex III of the Directive (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL see 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 Obligated Entity appears unusual or excessively complex given the nature of the Obligated Entity'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 unassociated third parties;
- (e) new products and new business practices, including new delivery mechanism, and the use of



EVERYTHING YOU NEED AND MORE

new or developing technologies for both new and pre-existing products;

(3) Geographical risk factors:

- (a) without prejudice to Article 64(1)(a), countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
- (b) countries identified by credible sources as having significant levels of corruption or other criminal activity;
- (c) countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
- (d) countries providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

9.17.2 The Obligated Entity examines, as far as reasonably possible, the background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose and in particular, obliged entities shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.

9.18 Clients from countries which inadequately apply FATF's recommendations

9.18.1 The FATF 40+9 Recommendations constitute the primary internationally recognized standards for the prevention and detection of Money Laundering and Terrorist Financing.

9.18.2 The Obligated Entity shall apply the following with respect to Clients from countries which inadequately apply FATF's recommendations:

- (a) exercise additional monitoring procedures and pay special attention to Business Relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or apply inadequately the aforesaid recommendations;
- (b) 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, business or investment background and purpose. If the Obligated Entity 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 4.2 of the Manual; and
- (c) with the aim of implementing the above, the Head of the Administration/Back-Office Department and the MLCO shall consult the country assessment reports prepared by the FATF (<http://www.fatf-gafi.org>), the other regional bodies that have been established and work on the principles of FATF [e.g. Moneyval Committee of the Council of Europe (www.coe.int/moneyval)] and the International Monetary Fund (www.imf.org). Based on the said reports, the MLCO

EVERYTHING YOU NEED AND MORE

assesses the risk from transactions and Business Relationships with persons from various countries and decides on the countries that inadequately apply the FATF's recommendations. According to the aforesaid decision of the MLCO, the Obligated Entity applies, when deemed necessary, enhanced due diligence measures for identifying and monitoring transactions of persons originating from countries with significant shortcomings and strategic deficiencies in their legal and administrative systems for the prevention of Money Laundering and Terrorist Financing.

9.19 Client Identification and Due Diligence Procedures (Specific Cases)

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

9.20 Natural persons residing in the Republic

9.20.1 The Obligated Entity 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) email address, if any;
- (e) date and place of birth;
- (f) nationality; and
- (a) details of the profession and other occupations of the Client including the name of employer/business organisation.

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

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

9.20.3 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 Obligated Entity 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.

- 9.20.4 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 Obligated Entity, 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.

9.21 Natural persons not residing in the Republic

- 9.21.1 The Obligated Entity shall obtain the information described in Section 9.18.1 to ascertain the true identity of the natural persons not residing in the Republic.
- 9.21.2 In addition to the information collected according to Section 9.18.1, without prejudice to the application on a risk-sensitive basis, the Obligated Entity 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.
- 9.21.3 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. 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 Obligated Entity 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.
- 9.21.4 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 Obligated Entity 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.

9.22 Joint accounts

In the cases of joint accounts of two or more persons, the identity of all individuals that hold or have the right to manage the account, are verified according to the procedures set in Sections 9.18.1 and 9.18.2 above.

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

In the case of accounts in the name of unions, societies, provident funds and charities, the Obligated Entity ascertains their purpose of operation and verifies their legitimacy by requesting the production of the articles and memorandum of association/procedure rules and registration



EVERYTHING YOU NEED AND MORE

documents with the competent governmental authorities (in case the law requires such registration).

Furthermore, the Obligated Entity 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 9.18.1 and 9.18.2.

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

- 9.24.1 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 9.18.1 and 9.18.2.
- 9.24.2 In addition, in the case of partnerships, the original or a certified true copy of the partnership's registration certificate shall be obtained.
- 9.24.3 The Obligated Entity shall obtain documentary evidence of the head office address of the business, ascertain the nature and size of its activities and receive all the information required according to Section 9.6 for the creation of the economic profile of the business.
- 9.24.4 The Obligated Entity shall request, in cases where it exists, the formal partnership agreement and shall also obtain mandate from the partnership authorising the opening of the account and confirming authority to a specific person who will be responsible for its operation.

9.25 Accounts of legal persons

- 9.25.1 For Clients that are legal persons, the Obligated Entity 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 9.18.1 and 9.18.2.
- 9.25.2 The Obligated Entity 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 9.18.1 and 9.18.2.
- 9.25.3 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:
 - 9.25.3.1 the registered number;
 - 9.25.3.2 the registered corporate name and trading name used;
 - 9.25.3.3 the full addresses of the registered office and the head offices;
 - 9.25.3.4 the telephone numbers, fax numbers and e-mail address;
 - 9.25.3.5 the members of the board of directors;



EVERYTHING YOU NEED AND MORE

9.25.3.6 the individuals that are duly authorised to operate the account and to act on behalf of the legal person;

9.25.3.7 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;

9.25.3.8 the registered shareholders that act as nominees of the Beneficial Owners; and

9.25.3.9 the economic profile of the legal person, according to the provisions of Section 9.6.

9.25.4 For the verification of the identity of the legal person, the Obligated Entity shall request and obtain,

among others, original or certified true copies of the following documents:

9.25.4.1 certificate of incorporation and certificate of good standing (where available) of the legal person;

9.25.4.2 certificate of registered office;

9.25.4.3 certificate of directors and secretary;

9.25.4.4 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;

9.25.4.5 memorandum and articles of association of the legal person;

9.25.4.6a 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;

9.25.4.7 in the cases where the registered shareholders act as nominees of the Beneficial Owners, a copy of the trust deed/agreement concluded between the nominee shareholder and the Beneficial Owner, by virtue of which the registration of the shares on the nominee shareholder's name on behalf of the Beneficial Owner has been agreed; and

9.25.4.8 documents and data for the verification, according to the procedures set in Sections 9.18.1 and 9.18.2., 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.

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

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

9.25.7 As an additional due diligence measure, on a risk-sensitive basis, the Obligated Entity 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 Obligated Entity's (legal person's) country of incorporation (for foreign companies) and/or request information from other sources in order to establish that the applicant Obligated Entity (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 Obligated Entity in the records of the Registrar of Companies and Official Receiver of the Republic or by an appropriate authority outside the Republic.

9.25.8 It is pointed out that, if at any later stage any changes occur in the structure or the ownership



EVERYTHING YOU NEED AND MORE

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 Obligated Entity for the legal person and all additional documentation and information for updating the economic profile of the legal person is collected.

- 9.25.9 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 Obligated Entity, 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.
- 9.25.10 Apart from verifying the identity of the Beneficial Owners, the Obligated Entity 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 Obligated Entity, 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.
- 9.25.11 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 Obligated Entity shall implement the following procedure.
- 9.25.11.1 the Obligated Entity 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 9.18.1 and 9.18.2;
- 9.25.11.2 furthermore, the Obligated Entity 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.

9.26 Investment funds, mutual funds and firms providing financial or investment services

- 9.26.1 The Obligated Entity 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 (see Appendix IV for the list of equivalent third countries), provided that the said persons:
- 9.26.1.1 possess the necessary license or authorisation from a competent supervisory/regulatory authority of the country of their incorporation and operation to provide the said services; and
- 9.26.1.2 are subject to supervision for the prevention of Money Laundering and Terrorist Financing purposes.



EVERYTHING YOU NEED AND MORE

- 9.26.2 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 Obligated Entity 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:
- 9.26.2.1 a copy of the license or authorisation granted to the said person from a competent supervisory/regulatory authority of its country of incorporation and operation, whose authenticity should be verified either directly with the relevant supervisory/regulatory authority or from other independent and reliable sources; and
- 9.26.2.2 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.
- 9.26.3 In the case of investment funds and mutual funds the Obligated Entity, 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.

9.27 Nominees or agents of third persons

- 9.27.1 The Obligated Entity 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 9.18.1 and 9.18.2 of the Manual:
- 9.27.1.1 the nominee or the agent of the third person, and
- 9.27.1.2 any third person on whose behalf the nominee or the agent is acting.
- 9.27.2 In addition, the Obligated Entity shall obtain a copy of the authorisation agreement that has been concluded between the interested parties.

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

- 9.28.1 The Obligated Entity is prohibited to rely on third parties established in high risk third countries for the customer due diligence measures and identification procedures.
- 9.28.2 The Obligated Entity may rely on third persons for the implementation of points (a), (b) and (c) of Client identification procedures and due diligence measures of Section 9.2 of the Manual, provided that:
- a. 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;

- b. the Obligated Entity applies the appropriate due diligence measures on the third person with respect to his professional registration and procedures and measures applied from the third person for the prevention of Money Laundering and Terrorist Financing, according to the provisions of the Directive; and
- c. the ultimate responsibility for meeting those requirements of Client identification and due diligence shall remain with the Obligated Entity who relies on the third person.

9.28.3 For the purposes of this Section of the Manual, third person means credit institutions or financial institutions or auditors or accountants or tax consultants or independent legal professionals or person providing trust and Obligated Entity services included in paragraphs (e) and (f) of the definition of the term “Other Business Activities”, falling under the EU Directive and are active in the Republic or in another country of the EEA which:

9.28.3.1 they are subject to mandatory professional registration, recognised by law, and

9.28.3.2 they subject to supervision regarding their compliance with the requirements of the EU Directive.

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

- a. Credit institutions or obliged entities that fall under the scope of the EU directive and are active within the EEA;
- b. Any third party conducting financial activities (as per the definition) operating outside the EEA which:
 - In accordance with a decision taken by the Advisory Authority for Combating Money Laundering and Terrorist Financing it has been determined that it applies requirements equivalent to those laid down in the European Union Directive;
 - Is subject to mandatory professional registration recognized by the law; and
 - Is subject to supervision with regard to its compliance with the said requirements

9.28.4 Further to point 2 above, third person for the purposes of this Section of the Manual may also be any other person who is engaged in financial business (as defined in Section 2 of the Law), or accountants or independent legal professionals or persons providing to third parties trust and Obligated Entity services as included in the definition of the term “Other Business Activities” and who operate in countries outside the EEA

and which according to a relevant decision of the Advisory Authority, have been determined that they impose equivalent procedures and measures for the prevention of Money Laundering and Terrorist Financing to those laid down by the EU Directive (see Appendix IV for the list of equivalent third countries).

It is provided that the abovementioned third persons have to fulfil the requirements set out in points 2(a) and 2(b) above.

- 9.28.5 The Obligated Entity may rely on third persons only at the outset of establishing a Business Relationship or the execution of an Occasional Transaction for the purpose of verifying the identity of their Clients. According to the degree of risk any additional data and information for the purpose of updating the Client's economic profile or for the purpose of examining unusual transactions executed through the account, is obtained from the natural persons (directors, Beneficial Owners) who control and manage the activities of the Client and have the ultimate responsibility of decision making as regards to the management of funds and assets.
- 9.28.6 Further to point 3 above, in the case where the third person of subparagraph (1) is an accountant or an independent legal professional or a trust and Obligated Entity services provider from a country which is a member of the EEA or a third country that the Advisory Authority has determined to be applying procedures and measures for the prevention of Money Laundering and Terrorist Financing equivalent to the EU Directive (see Appendix IV for the list of equivalent third countries), then the Obligated Entity, before accepting the Client identification data verified by the said third person, shall apply the following additional measures/procedures:
- 9.28.6.1 the MLCO or the appointed person shall assess and evaluate, according to point (l) of Section 4.2 of this Manual, the systems and procedures applied by the third person for the prevention of Money Laundering and Terrorist Financing, as applicable;
- 9.28.6.2 as a result of the assessment of point (a) above, the MLCO must be satisfied that the third person implements Client identification and due diligence systems and procedures which are in line with the requirements of the Law and the Directive;
- 9.28.6.3 the MLCO shall maintain a separate file for every third person of the present paragraph, where it stores the assessment report of point (a) and other relevant information (for example identification details, records of meetings, evidence of the data and information of point 2 above); and
- 9.28.6.4 the commencement of the cooperation with the third person and the acceptance of Client identification data verified by the third person is subject to approval by the MLCO, according to point (l) of Section 4.2 of the Manual.



EVERYTHING YOU NEED AND MORE

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

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

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

10. On Going Monitoring

10.1. General

The Obligated Entity has a full understanding of normal and reasonable account activity of its Clients as well as of their economic profile and has the means of identifying transactions which fall outside the regular pattern of an account's activity or to identify complex or unusual transactions or transactions without obvious economic purpose or clear legitimate reason. Without such knowledge, the Obligated Entity shall not be able to discharge its legal obligation to identify and report suspicious transactions to the Unit, according to point (g) of Section 4.2 and Section 11 of the Manual.

The constant monitoring of the Clients' accounts and transactions is an imperative element in the effective controlling of the risk of Money Laundering and Terrorist Financing. In this respect, the MLCO shall be responsible for maintaining as well as developing the on-going monitoring process of the Obligated Entity. The AMLCO monitors the clients' accounts on a weekly basis. The AMLCO goes through the clients CRM profile and monitors their KYC documents and their test of appropriateness. The AMLCO further monitors the client's transactions if the amount invested is in accordance with the information stated in their economic profile and in the client's details. The AMLCO is in collaboration with the Head of Back Office and Safekeeping and ensures that the client's deposits and withdrawals are completed through the same bank account.

The Internal Auditor shall review the Obligated Entity's procedures with respect to the on-going monitoring process, at least annually.

10.2. Procedures

The Firm's approach to assessing and managing the ML/TF risk associated with business relationships and occasional transactions should include the following:

- Business-wide risk assessments – which should help the firm understand where it is exposed to ML/TF risk and which areas of its business it should prioritise in the fight against ML/TF. Furthermore, and in line with Article 8 of Directive (EU) 2015/849, the firm should identify and assess the ML/TF risk associated with the products and services it offers, the jurisdictions it operates in, the customers they



EVERYTHING YOU NEED AND MORE

attract and the transaction or delivery channels it uses to service its customers.

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

The identification of:

- all high-risk Clients, as applicable; the Obligated Entity shall be able to produce detailed lists of high risk Clients, so as to facilitate enhanced monitoring of accounts and transactions, as deemed necessary;
- The Obligated Entity shall treat all of its clients as high-risk clients
- Identify the customer and, where applicable, the customer's beneficial owner or legal representatives;
- Verify the customer's identity on the basis of reliable and independent sources and, where applicable, verify the beneficial owner's identity in such a way that the Obligated Entity is satisfied that it knows who the beneficial owner is; and
- Establish the purpose intended nature of the business relationship

The Firm should furthermore, gather sufficient information in regards to:

- 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; and
 - 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 Dealing Department) shall be responsible to communicate with the MLCO;
 - suspicious transactions and screening of all Clients through the "World compliance check" or equivalent software for passport verification, PEP Research, sanctions lists, profile checking and risk assessment.
 - further to point (a) above, the investigation of unusual or suspicious transactions by the MLCO. The results of the investigations are recorded in a separate memo and kept in the file of the Clients concerned;
- the ascertainment of the source and origin of the funds credited to accounts; and
 - 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 MLCO, 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 Obligated Entity's

EVERYTHING YOU NEED AND MORE

- 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 (geographic area), the source of the funds, the type of transaction, the products the client invested to, the transactions or bank service delivery channels or other risk factors. The Obligated Entity shall pay particular attention to transactions exceeding the abovementioned limits, which may indicate that a Client might be involved in unusual or suspicious activities; and
 - iv. 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 Obligated Entity as well as dormant accounts exhibiting unexpected movements.
 - v. The Obligated Entity is prohibited from accepting any amount equal 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 with:
 - a) Persons trading in precious stones and/or precious metals,
 - b) Persons trading in mechanical vehicles,
 - c) Persons trading in works of art and/or antiques.

The breach of the said prohibition consists a criminal offence

11. Recognition & Reporting of Suspicious Transactions /Activities to The Unit

11.1 Reporting of Suspicious Transactions to the Unit

The Obligated Entity, in cases where there is an attempt of executing transactions which it knows or suspects that are related to money laundering or terrorist financing, reports, through the MLCO its suspicion to the Unit in accordance with point (g) of Section 6.2 and this section. In accordance with Circular C058, all reporting entities should submit Suspicious Activities Reports and Suspicious Transactions Reports only online via the new procedure that will be based on a sophisticated and highly secure IT system implemented by MOKAS, namely “goAML Professional Edition (PE)”. The Obligated Entity is registered with the goAML IT System in order to report any suspicious activities and transactions when necessary.

11.2 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 Obligated Entity has created for the Client. The Obligated Entity shall ensure that it maintains adequate information and knows enough about its Clients' activities in order to recognize 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 III 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 Obligated Entity and its employees (especially the MLCO and the Brokerage Department) in recognizing the main methods used for Money Laundering and Terrorist Financing. The detection by the Obligated Entity of any of the transactions contained in the said list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds, the nature and economic/business purpose of the underlying transaction, and the circumstances surrounding the particular activity.
3. In order to identify suspicious transactions, the MLCO shall perform the following activities:
 - monitor on a continuous basis any changes in the Client's financial status, business activities, type of transactions etc.
 - monitor on a continuous basis if any Client is engaged in any of the practices described in the list containing examples of what might constitute suspicious transactions/activities related to Money Laundering and Terrorist Financing which is mentioned in Appendix III of this Manual.

Furthermore, the MLCO shall perform the following activities:

- receive and investigate information from the Obligated Entity'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 4.2 of the Manual. The said reports are archived by the MLCO;
- evaluate and check the information received from the employees of the Obligated Entity, with reference to other available sources of information and the exchanging of information in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained on the report which is submitted to the MLCO is evaluated on the Internal Evaluation Report according to point (f) of Section 5.2 of the Manual, which is also filed in a relevant file;
- if, as a result of the evaluation described above, the MLCO decides to disclose this information to the Unit, then he prepares a written report, which he submits to the Unit, according to point (f) of Section 4.2 and Section 11.4 of the Manual; and
- if as a result of the evaluation described above, the MLCO decides not to disclose the relevant information to the Unit, then he fully explain the reasons for his decision on the Internal Evaluation Report.

11.3 MLCO's Report to the Unit

All the reports of the MLCO of point (g) of Section 4.2 of the Manual are submitted to MOKAS via the goAML IT System.

After the submission of a suspicion report to Unit, the Obligated Entity may subsequently wish to terminate its relationship with the Client concerned for risk avoidance reasons. In such an event, the Obligated Entity 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 (g) of Section 4.2 of the Manual, the Obligated Entity 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 Obligated Entity 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 Obligated Entity and its employees.

Furthermore, after the submission of a suspicion report of point (g) of Section 4.2 of the Manual, the Clients' accounts concerned as well as any other connected accounts are placed under the close monitoring of the MLCO.

11.4 Submission of Information to the Unit

The Obligated Entity shall ensure (see also Section 12 of the Manual) that in the case of a suspicious transaction investigation by the Unit, the MLCO 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; and
 - vi. the form of instructions and authorisation that have been given the type and identifying number of any account involved in the transaction.

12. Record-Keeping Procedures

12.1 General

The Administration/Back-Office Department of the Obligated Entity shall maintain records of:

- a. the Client identification documents and information obtained during the Client identification and due diligence procedures, as applicable; and
- b. the details of all relevant records with respect to the provision of investment services to Clients

The documents/data mentioned above shall be kept for a period of at least 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 Obligated Entity until the Unit confirms that the investigation has been completed and the case has been closed.

12.2 Format of Records

The Administration/Back-Office Department may retain the documents/data mentioned in Section 12.1 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 Obligated Entity will establish a documents/data retention policy, the MLCO 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 Obligated Entity to the above, at least annually.

12.3 Certification and language of documents

1. The documents/data obtained, shall be in their original form or in a certified true copy form. In the case that the documents/data are certified as true by a different person than the Obligated Entity itself or by the third person mentioned in Section 9.26, the documents/data must be apostilled or notarised.
2. Copy of the original documents/data obtained are accepted provided that at least one of the conditions mentioned under sub-paragraph (a) is followed:
 - (a) In addition to the measure under section 64(1)(a)(ii) of the Law 188(I)/2007, practical procedures that can be applied as implementing measures of section 64(1)(a)(i) and (ii) of the Law 188(I)/2007 regarding non face to face customers of the Obligated Entity are the following:
 - i. Ensure that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution which operates in a country within the European Economic Area or in a third country that the Advisory Authority for Combating Money Laundering and Terrorist Financing has determined to be applying procedures and measures for the prevention of money laundering and terrorist financing equivalent to the European Union Directive.
 - ii. Obtain direct confirmation for the establishment of a business relationship via the direct personal contact, regarding the prospective customer's true name, address and passport / identity card number (only for residents of the Republic of Cyprus) from a credit institution or financial institutions that the client collaborates with, that operates in a Member State or in a third country that the Advisory Authority for Combating Money Laundering and

Terrorist Financing has determined to be applying procedures and measures for the prevention of money laundering and terrorist financing equivalent to the European Union Directive (or a certified true copy of the confirmation).

- iii. Contact the customers via telephone at their residence or office, before the establishment of a business relationship or the occasional transaction, on a telephone number which has been verified from a reliable and independent source. During the telephone correspondence, the Obligated Entity shall verify other information submitted by the customers during the account opening procedure.
- iv. Contact the customers via video call, provided that the safeguards of video recording and screen shot of the conversation are ensured. It is provided that in case where the verification of the customers / beneficial owners' identity has been completed based on the provisions of the respective paragraph, the cumulative amount of deposited funds of customers / beneficial owners should not exceed €2,000, irrespective of the number of accounts the customers / beneficial owners hold with the Obligated Entity, in case where no additional measures of this section or of the article 64(1)(a)(ii) of the Law 188(I)/2007, have been taken.

It is provided that the Obligated Entity is required to implement appropriate measures and procedures in order to:

1. Verify and monitor the amount deposited by the customer as well as the risk of money laundering and terrorist financing or terrorist financing operations and applies enhanced measures for the verification of customer's identity, depending on the degree of risk.
 2. Ensure the normal conduct of business in case where the cumulative amount of deposited funds of customers /beneficial owners has not exceed €2,000 annually.
 3. Warn its customers appropriately and sufficiently in due time regarding the above procedure and receive their explicit consent as to the procedure that is to be followed, before the establishment of the business relationship.
- v. Contact the customer via email at an email address which has been verified from a reliable and independent source, through registered mail (for example, the correspondence may include documents required for the account opening, which the customers must return to the Obligated Entity or a password that the customers require to access their online account).
 - vi. Verify the customers' identity via electronic means:

1. The verification of the customers' identity via electronic means is performed by the Obligated Entity or by a third person. All the following conditions, cumulatively are satisfied by the Obligated Entity and the third person:
 - i. The online databases that the third person or the Obligated Entity has access, is registered in, and / or approved by the Commissioner for the Protection of Personal Data for the purpose of maintaining personal data (or the competent authority in the country that the database is maintained).
 - ii. The online databases provide access to information regarding both current and past statements indicating that indeed the person existed and contains both positive information (as a minimum the full name, address and the customers' date of birth) and negative information (e.g. committing crimes like identity theft, included in deceased persons lists, included in sanctions lists and restrictive measures issued by the Council of the European Union and the UN Security Council).
 - iii. The electronic databases contain a wide range of sources with information from various time intervals, which are updated in real time and trigger alerts when important data are differentiated.
 - iv. Transparent procedures have been implemented, which enable the Obligated Entity to know what information has been investigated, what are the results and their significance in relation to the degree of certainty with respect to the verification of the customer.
 - v. Procedures have been established that enable the Obligated Entity to record and maintain information used and the results in regards to the verification of customers' identity.
2. The Obligated Entity evaluates the results of the verification of customers' identity via electronic means in order to ensure that the provisions of article 61(3) of the Law 188(I)/2007 are satisfied. The Obligated Entity establishes mechanisms for the implementation of quality controls in order to assess the quality of information that the Obligated Entity intends to rely on.
3. The information should be derived from two or more sources. As a minimum, the verification procedure via electronic means shall meet the following correlation model:
 - i. identification of the customers' full name and current address using the same source, and
 - ii. identification of the customers' full name and either their current address or date of birth using a different source.
4. For the purposes of the verification of customers' identity via electronic means, the Obligated Entity must establish procedures so as to ensure the completeness, accuracy and reliability of the information obtained. It is

provided that the results of the verification process should include both positive and negative 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 or English.

Each time the Obligated Entity 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.

12.4 True Translation

The Obligated Entity's Policy is to keep documents provided for by the Obligated Entity's clients to meet business and regulatory requirements and any other documentation including, but not limited to, contracts, agreements, official correspondence and other legal or non-legal documentation in either English or Greek language.

Therefore, documents received in languages other than Greek or English are translated either internally by an employee who is fluent in English and in the language of the translated document or through a professional translator.

Exact and full translation is required including any stamps and any other phrases or indicators not included in the main body of the document.

The translator shall put the date and his signature on the translated document. The original document and its translation shall be kept together in electronic form in the clients file concerned. Documents other than those referred or related to a customer shall be kept either in electronic format or in hard copy.

13. Employees' Obligations, Education And Training

13.1 Employees' Obligations

- a. The Obligated Entity'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 to point (e) of Section 4.2, 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; and
- c. according to the Law, the Obligated Entity's employees shall fulfil their legal obligation to report their suspicions regarding Money Laundering and Terrorist Financing, after their compliance with point (b) above.

13.2 Education and Training

- a. The Obligated Entity shall ensure that its employees are fully aware of their legal obligations according to the Law and the Directive, by introducing a complete employees' education and training program;
- b. the timing and content of the training provided to the employees of the various departments will be determined according to the needs of the Obligated Entity. 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;
- c. the training program aims at educating the Obligated Entity's employees on the latest developments in the prevention of Money Laundering and Terrorist Financing, including the practical methods and trends used for this purpose;
- d. the training program will have a different structure for new employees, existing employees and for different departments of the Obligated Entity 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; and
- e. The MLCO 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

13.3 MLCO Education and Training Program

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

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

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

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

14. FATCA & CRS Reportable Information: General Requirements

The Obligated Entity shall ensure that carries out the due diligence processes for identifying reportable accounts for account holders that are resident in CRS Reportable Jurisdictions outside of the EU, as set out in the CRS regulations.

The Obligated Entity is obliged to review and collect details of accounts held by persons that are tax resident elsewhere and report this to the Cyprus Tax Department for onward transmission under the exchange of information articles in the various treaties and conventions to which Cyprus is party.

Although, the Obligated Entity does not accept US-Reportable clients, it has nevertheless updated its questionnaire accordingly so it complies with the CRS/FATCA reporting obligations.

A US Person, according to FATCA's glossary, means:

- An individual who is a US citizen or US resident alien
- A partnership, corporation, Obligated Entity, or association created or organized in the US or under the Laws of the US
- An estate (other than a foreign estate), or
- A domestic trust

The Obligated Entity's Back Office Department, through its questionnaire, requires from its clients the following information:

- a. Name
- b. Date and place of birth
- c. Address
- d. Taxpayer Identification Number(s) (TIN)
- e. Jurisdiction(s) of residence
- f. The account number (or a functional equivalent in the absence of an account number)
- g. The name and identifying number of the reporting financial institution
- h. The account balance or value as of the end of the calendar year or other appropriate period.

Due Diligence requirements apply to "new" accounts and "pre-existing" accounts.

The Obligated Entity shall identify, maintain and report information on the tax residence of Account holders, and for FATCA purposes whether they are US citizens, irrespective of whether or not they are tax resident in a Reportable Jurisdiction, as required per the regulations. This is referred to as the "wider approach".



EVERYTHING YOU NEED AND MORE

The Obligated Entity is required to carry out due diligence procedures on its account holders, in order to establish if the person holding the account is tax resident in a jurisdiction with which Cyprus has agreed to automatically exchange information.

An account is treated as a Reportable account as of the date it is identified as such pursuant to the due diligence procedures that financial institutions must follow.

The Obligated Entity's Back Office Department shall be responsible for the collection and monitoring of the required information which shall be under the supervision of the Obligated Entity's Compliance Officer.

The Obligated Entity shall keep records of the required information for the maximum period of 5 years from the end of the business relationship between the Obligated Entity and its clients.

The Obligated Entity complies and shall ensure compliance with the FATCA regulations, the European Commission's and CySEC's Regulations in regards to Banned Countries, High-Risk Countries and shall keep records of the updated High-Risk Countries, Banned Countries List which it shall also share with the Obligated Entity's employees and ensure their acknowledgement.

15. General Data Protection

The new General Data Protection Regulation (GDPR) came into effect on the 25th of May 2018.

GDPR is a new European data protection law which requires immediate individual implementation in each Member State. The Regulation applies to controllers and processors in the EU irrespective of where the processing takes place and it applies to processing activities that are related to goods or services, irrespective of whether payment is required and the monitoring of data subjects' behavior within the EU. It also applies to controllers not in the EU, but where Member State law applies.

It sets new stricter standards to protect your personal data¹, to respect your privacy and for us to process² only the data necessary to efficiently deliver our services to you.

We have aligned our Privacy Policy and our Cookies Policy to reflect the GDPR requirements. You can review our updated Privacy Policy for guidance on your rights relating to the information we hold about you.

Please find our Obligated Entity's policies available for your perusal on both our website and the CRM (Portal).

¹ Personal Data means any information relating to an identified or identifiable natural person ("data subject").

² Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.



EVERYTHING YOU NEED AND MORE

Appendix I

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 MLCO USE

Date Received: Time Received: Ref.



EVERYTHING YOU NEED AND MORE

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

Appendix II

INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

Reference: Client's Details:

Informer: Department:

INQUIRIES UNDERTAKEN (Brief Description)

.....

.....

.....

ATTACHED DOCUMENTS

.....

.....

.....

.....

MLCO DECISION

.....

.....

.....

FILE NUMBER:



EVERYTHING YOU NEED AND MORE

MLCO SIGNATURE:..... DATE:.....

Appendix III

Examples Of Suspicious Transactions/Activities Related To Money Laundering And Terrorist Financing

A. Money Laundering

- a. Transactions with no discernible purpose or are unnecessarily complex.
- b. 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.
- c. The transactions or the size of the transactions requested by the Client do not comply with his usual practice and business activity.
- d. 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.
- e. The Business Relationship involves only one transaction or it has a short duration.
- f. There is no visible justification for a Client using the services of a particular obliged entity. For example the Client is situated far away from the

particular obliged entity and in a place where he could be provided services by another obliged entity.

- g. There are frequent transactions in the same financial instrument without obvious reason and in conditions that appear unusual (churning).
- h. 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.
- i. Any transaction the nature, size or frequency appear to be unusual, e.g. cancellation of an order, particularly after the deposit of the consideration.
- j. 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.
- k. The settlement of any transaction but mainly large transactions, in cash.
- l. Settlement of the transaction by a third person which is different than the Client which gave the order.
- m. Instructions of payment to a third person that does not seem to be related with the instructor.
- n. 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.
- o. 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 obliged entity's,

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 obliged entity to verify.

- p. A Client provides unusual or suspicious identification documents that cannot be readily verified.
- q. A Client's home/business telephone is disconnected.
- r. A Client that makes frequent or large transactions and has no record of past or present employment experience.
- s. Difficulties or delays on the submission of the financial statements or other identification documents, of a Client/legal person.
- t. A Client who has been introduced by a foreign obliged entity, 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.
- u. 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.).
- v. The stated occupation of the Client is not commensurate with the level or size of the executed transactions.
- w. 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.

- x. 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).
- y. Complex trust or nominee network.
- z. Transactions or Obligated Entity 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.
- aa. Use of general nominee documents in a way that restricts the control exercised by the Obligated Entity's board of directors.
- bb. Changes in the lifestyle of employees of the obliged entity, e.g. luxurious way of life or avoiding being out of office due to holidays.
- cc. Changes the performance and the behaviour of the employees of the obliged 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:

- a. Establishing a non-profit organisation with a specific charitable purpose but which actually exists only to channel funds to a terrorist organisation.
 - b. 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.
 - c. The non-profit organisation serves as an intermediary or cover for the movement of funds on an international basis.
 - d. The non-profit organisation provides administrative support to the terrorist movement.
- ii. Unusual characteristics of non-profit organisations indicating that they may be used for an unlawful purpose are the following:
 - a. Inconsistencies between the apparent sources and amount of funds raised or moved.
 - iii. A mismatch between the type and size of financial transactions and the stated purpose and activity of the non-profit organisation.
 - iv. A sudden increase in the frequency and amounts of financial transactions for the account of a non-profit organisation.
 - v. Large and unexplained cash transactions by non-profit organisations.
 - vi. The absence of contributions from donors located within the country of origin of the non-profit organization.

APPENDIX IV

BANNED JURISDICTIONS

Banned Jurisdictions shall mean those countries which do not comply with international laws, specifically laws for combating Money Laundering and Terrorist Financing and are sanctioned by the U.N and/or EU and/or other International Organizations.

Non-Exhaustive List of the High Risk Jurisdictions:

Albania
The Bahamas
Barbados
Botswana
Cambodia
Ghana
Jamaica
Mauritius
Myanmar
Nicaragua
Pakistan
Panama
Syria
Uganda
Yemen
Zimbabwe

Banned Jurisdictions:

Democratic People's Republic of Korea (DPRK)

And any other country which comes under these sanctions.

However, according to CySEC regulations, clients can only be accepted from EU countries and from any other third not banned country after taking authorization from the Financial Authorities of the country or obtaining the relevant legal opinion.

The Directive (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 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 Commission Directive 2006/70/EC provides Annex II and Annex III which lays a non-exhaustive list of factors for lower and higher risk.

ANNEX II

The following is a non-exhaustive list of factors and types of evidence of potentially lower risk referred to in Article 16:

(1) Customer risk factors:

- (a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
- (b) public administrations or enterprises;
- (c) customers that are resident in geographical areas of lower risk as set out in point (3);

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

- (a) life insurance policies for which the premium is low;
- (b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
- (c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;
- (d) financial products or services that provide appropriately defined and limited 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 (e.g. 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.

ANNEX III

The following is a non-exhaustive list of factors and types of evidence of **potentially higher risk** referred to in Article 18(3):

(1) Customer risk factors:

- (a) the business relationship is conducted in unusual circumstances;
- (b) customers that are resident in geographical areas of higher risk as set out in point (3);
- (c) legal persons or arrangements that are personal asset-holding vehicles;
- (d) companies that have nominee shareholders or shares in bearer form;
- (e) businesses that are cash-intensive;
- (f) the ownership structure of the Obligated Entity appears unusual or excessively complex given the nature of the Obligated Entity'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 unassociated 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 9, 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 European Union or the United Nations;
- (d) countries providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.