PREVENTION OF MONEY LAUNDERING & TERRORIST FINANCING MANUAL

Previous Version Date:	January 2017
Current Version:	October 2018
Approved by:	Board of Directors

Table of contents

1 GENERAL DEFINITIONS

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

"**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 the natural person or natural persons, who ultimately owns or control the Client and/or the natural person on whose behalf a transaction or activity is being conducted. The Beneficial Owner shall at least include: (a) In the case of corporate entities: the natural person who ultimately owns or controls a corporate entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that corporate entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with European Union law or subject to equivalent international standards which ensure adequate transparency of ownership information. Provided that: (a) an indication of direct shareholding shall be a shareholding of 25% plus one share or an ownership interest of more than 25% in the client held by a natural person; and (b) an indication of indirect ownership shall be a shareholding of 25% plus one share or an ownership interest of more than 25% in the client held by a corporate entity, which is under the control of a natural person, or by multiple corporate entities, which are under the control of the same natural person or persons. Provided further that the control by other means can be verified, inter alia, based on the criteria provided for in section 142 (1) (b) (annual and consolidated financial statements)and section 148 (parent and subsidiary companies)of the Companies Law; the natural person who holds the position of senior managing official if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under sub paragraph (i) of the present paragraph is identified, or if there is any doubt that the person identified is the beneficial owner:

	Provided that the Company shall keep record of the actions taken in order to identify the beneficial ownership under sub paragraphs (i) and (ii); (b) in the case of trusts: (i) the settlor; (ii) the trustee or commissioner; (iii) the protector, if any; (iv) the beneficiary, or where the individual benefiting from the legal arrangement or legal entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates; (v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means; and (c) in the case of legal entities, such as foundations, and legal arrangements similar to trusts, the natural person holding equivalent or similar positions to the person referred to in paragraph (b).
"**Business Relationship**"	means a business, professional or commercial relationship which is connected with the professional activities of the Company and which was expected, at the time when the contact was established, to have an element of duration;
"**Client**" or "**Customer**"	means any legal or physical person aiming to conclude a Business Relationship or conduct an occasional transaction with the Company;
"**Company**"	means Leverate Financial Services Ltd which is incorporated in the Republic of Cyprus with registration number HE290182 and regulated by Cyprus Securities and Exchange Commission with license number 160/11;
"**Directive**"	Directive DI144-2007-08 of the CySEC for the Prevention of Money Laundering and Terrorist Financing as this is amended from time to time;
"**EU Directive**"	means an act of the European Union entitled 'Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 relating to the prevention of the use of the credit and financial system for money laundering and financing of terrorism, the amendment of regulation (EU) number 648/2012 of the European Parliament and of the Council, and repealing directive 2005/60/EC of the European Parliament and of the Council and directive 2006/70/EC of the Commission.
"**Laundering Offences**"	shall include the circumstances where a person who knows or ought to have known that any kind of property constitutes proceeds from the commission of illegal activities, carries out the following activities: (i) converts or transfers or removes such property, for the purpose of concealing or disguising its illicit origin or of assisting in any way any person who is involved in the commission of the predicate offence to

	carry out any of the above actions or acts in any other way in order to evade the legal consequences of his actions; (ii) conceals or disguises the true nature, the source, location, disposition, movement of and rights in relation to, property or ownership of this property; (iii) acquires, possesses or uses such property; (iv) participates in, associates, co-operates, conspires to commit, or attempts to commit and aids and abets and provides counselling or advice for the commission of any of the offences referred to above; (v) provides information in relation to investigations that are carried out for laundering offences for the purpose of enabling the person who acquired a benefit from the commission of a predicate offence to retain the proceeds or the control of the proceeds from the commission of the said offence.
"**Law**"	means the Prevention and Suppression of Money Laundering and Terrorist Financing Law (188(I)/2007) as this is amended from time to time.
"**Manual**"	means the Company's Prevention of Money Laundering & Terrorist Financing Manual (this manual);
"**Occasional Transaction**"	means any transaction other than a transaction carried out in the course of the business relationship with the Company;
"**Politically exposed person**" ("**PEP**")	means a natural person who is or who has been entrusted with prominent public functions in the Republic of Cyprus or in another country, an immediate close relative of such person as well as a person known to be a close associate of such person: Provided that, for the purpose of the present definition, "**prominent public function**" means any of the following public functions: 1. heads of State, heads of government, ministers and deputy or assistant ministers; 2. members of parliament or of similar legislative Boardies; 3. members of the governing Boardies of political parties; 4. members of supreme courts, of constitutional courts or of other high-level judicial Boardies, the decisions of which are not subject to further appeal, except in exceptional circumstances; 5. members of courts of auditors or of the boards of central banks; 6. ambassadors, chargés d'affaires and high-ranking officers in the armed forces; 7. members of the administrative, management or supervisory Boardies of State-owned enterprises; 8. directors, deputy directors and members of the board or equivalent function of an international organisation;

	9. mayor: Provided further that no public function referred to in points (a) to (i) shall be understood as covering middle-ranking or more junior officials; Provided furthermore that "**close relatives of a politically exposed person**" includes the following: (a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; (b) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person; (c) the parents of a politically exposed person; Provided even furthermore that "persons known to be close associates of a politically exposed person" means natural person: (a) who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person; (b) who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.
"**Predicate offences**"	are defined as any offence which is defined as a criminal offence by a law of the Republic of Cyprus;
"**Shell bank**"	means a credit institution or financial institution, or an institution that carries out activities equivalent 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;
"**Suspicious transactions**":	include in general transactions that will often be one which is inconsistent with a Client's known, legitimate business or personal activities or with the normal business of the specific account, or in general with the economic profile that the Company has created for the Client. A list of relevant examples is included in Appendix A;
"**Terrorist financing**"	means the provision or gathering of funds by any means, directly or indirectly, with the intention to use such funds or knowing that they will be used in whole or in part for the commission of an offence within the meaning given to the term by section 4 of the International Convention for the Suppression of the Financing of Terrorism (Ratification and Other Provisions) Law and by sections 5 to 13 of the Combating of Terrorism Law;
"**Unit for Combating Money Laundering Offences**" ("**MOKAS**")	means the competent national authority responsible inter alia for receiving, requesting, analyzing and disseminating disclosures of suspicious transactions reports and other relevant information concerning suspected money laundering or financing of terrorism activities;

2 INTRODUCTORY NOTES

This Manual sets out the general principles, obligations and procedures that the Company's employees should follow at all times for compliance with the legislative and regulatory provisions for the prevention and combatting money laundering and terrorist financing. This Manual should be read in conjunction with the Internal Operations Manual ("IOM") in relation inter alia to the provisions for account opening and relevant policies including the Client Acceptance Policy.

The Manual is developed and periodically updated by the Anti Money Laundering Compliance Officer (hereinafter the "AMLCO") based on the general principles set up by the Company's Board of Directors (hereinafter the "Board") in relation to the prevention of Money Laundering and Terrorist Financing.

All amendments and/or changes of the Manual are approved by the Board.

Any questions in relation to this Manual should be addressed to the AMLCO.

3 THE RESPONSIBILITIES OF THE BOARD OF DIRECTORS

The Board is responsible for determining, recording and approving the Company's general policy principles in relation to the Prevention of Money Laundering and Terrorist Financing. The Board is also responsible for the appointment of the Company's AMLCO and for establishing their duties and responsibilities, which should be clearly stated in the Company's IOM.

The responsibilities of the Board include further the following:

a) Approves the Manual which is communicated to all employees of the Company, that manage, monitor or control in any way the Clients' transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined.

b) Ensures that all requirements of the Law, especially article's 58 in relation to the procedures for preventing Money Laundering and Terrorist Financing, and of the Directive are applied, and assures that appropriate, effective and sufficient systems and controls are introduced for achieving the abovementioned requirement.

c) Assures that the AMLCO and his assistants and any other person who has been assigned with the duty of implementing the procedures for the prevention of money laundering and terrorist financing, have complete and timely access to all data and information concerning clients' identity, transactions' documents and other relevant files and information maintained by the Company so as to be fully facilitated in the effective execution of their duties.

d) Ensures that all employees are aware of the person who has been assigned the duties of the AMLCO, as well as his assistants, 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.

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

f) Ensures that the AMLCO has sufficient resources, including competent staff and technological equipment, for the effective discharge of his duties.

g) Assesses and approves the Annual Report and takes all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the Annual Report.

4 OBLIGATIONS OF THE INTERNAL AUDITOR

The Company, taking into account the nature, scale and complexity of its business activities, as well as the nature and the range of its investment services and activities, has outsourced the internal audit function through the appointment of qualified and experienced Internal Auditors.

The Internal Auditor reviews and evaluates, 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. The findings and observations of the Internal Auditor are submitted, in a written report form, to the Board which decides the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected. The minutes of the abovementioned decision of the Board and the Internal Auditor's report are submitted to CySEC within twenty (20) days from the date of the relevant meeting and no later than four (4) months after the end of the calendar year.

5 THE AMLCO

5.1 **Duties**

1. The AMLCO shall belong hierarchically to the higher ranks of the Company's organizational structure so as to command the necessary authority.
2. The duties of the AMLCO shall include, inter alia, the following:
   a) Designs, based on the general policy principles determined by the Board, the internal practice, measures, procedures and controls relevant to the prevention of money laundering and terrorist financing, and describes and explicitly allocates the appropriateness and the limits of responsibility of each department that is involved in the abovementioned.

      It is provided that, the above include measures and procedures for the prevention of the abuse of new technologies and systems providing financial services, for the purpose of money laundering and terrorist financing (e.g. services and transactions via the internet or the telephone), as well as measures so that the risk of money laundering and terrorist financing is appropriately considered and managed in the course of daily activities of the Company with regard to the development of

new products and possible changes in the Company's economic profile (e.g. penetration into new markets).

b) Develops and establishes the Client Acceptance Policy, and submits it to the Board for consideration and approval.

c) Responsible for the preparation of the Manual.

d) Monitors and assesses the correct and effective implementation of the policy, the practices, measures, procedures and controls and in general the implementation of the Manual. In this regard, applies appropriate monitoring mechanisms (e.g. on-site visits to different departments of the Company which will provide him all the necessary information for assessing the level of compliance of the departments and employees of the Company with the procedures and controls which are in force. In the event that he 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) Receives information from the Company's employees which is considered to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities. The information is received in a written report form (hereinafter to be referred to as "Internal Suspicion Report"), a specimen of such report is attached in Appendix B.

f) Evaluates and examines the information received as per point (e), by reference to other relevant information and discusses the circumstances of the case with the informer and, where appropriate, with the informer's superiors. The evaluation of the information of point (e) is been done on a report (hereinafter to be referred to as "Internal Evaluation Report"), a specimen of which is attached in Appendix C.

g) If following the evaluation described in point (f), the AMLCO decides to notify MOKAS, then he completes a written report and submit it to MOKAS the soonest possible. A specimen of such report (hereinafter to be referred to as "AMLCO's Report to the Unit for Combating Money Laundering") is attached to Appendix D. It is provided that, after the submission of the AMLCO's report to MOKAS, the accounts involved and any other connected accounts, are closely monitored by the AMLCO and following any directions from MOKAS, thoroughly investigates and examines all the transactions of the accounts.

h) If following the evaluation described in point (f) the AMLCO decides not to notify MOKAS, then he fully explains the reasons for such a decision on the "Internal Evaluation Report" which is attached in Appendix C.

i) Acts as the first point of contact with MOKAS, upon commencement and during an investigation as a result of filing a report to MOKAS according to point (g).

j) Ensures the preparation and maintenance of the lists of clients categorised following a risk based approach, which contains, inter alia, the names of clients, their account number and the date of the

commencement of the business relationship. Moreover, ensures the updating of the said lists with all new or existing clients, in the light of additional information obtained.

k) Detects, records, and evaluates, at least on an annual basis, all risks arising from existing and new clients, new financial instruments and services and updates and amends the systems and procedures applied by the Company for the effective management of the aforesaid risks.

l) Evaluates the systems and procedures applied by a third person on whom the Company relies for client identification and due diligence purposes and approves the cooperation with it.

m) Ensures that the branches and subsidiaries of the Company that operate in countries outside the European Economic Area, have taken all necessary measures for achieving full compliance with the provisions of the Directive, in relation to client identification, due diligence and record keeping procedures.

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

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

p) Determines the Company's departments and employees that need further training and education for the purpose of preventing money laundering and terrorist financing and organises appropriate training sessions/seminars. In this regard, prepares and applies an annual staff training program. Assesses the adequacy of the education and training provided.

q) Prepares correctly and submits timely to CySEC the monthly prevention statement and provides the necessary explanation to the appropriate employees of the Company for its completion.

r) Prepares the annual report as per section 5.2. of this Manual.

s) Responds to all requests and queries from MOKAS and CySEC, provides all requested information and fully cooperates with MOKAS and CySEC.

t) Maintains a registry which includes the reports of points (e), (f) and (g), and relevant statistical information (department that submitted the internal report, date of submission to the AMLCO, date of assessment, date of reporting to MOKAS), the evaluation reports of point (d) and all the documents that verify the accomplishment of his duties specified in the present subparagraph.

3. During the execution of his duties and the control of the compliance of the Company with the Law and the Directive, the AMLCO obtains and utilises data, information and reports issued by international organizations including the following:

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

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

(c) the EU Common Foreign & Security Policy (CFSP)- https://eeas.europa.eu/topics/sanctions-policy/8442/consolidated-list-of-sanctions_en

(d) the UN Security Council Sanctions Committees - www.un.org/sc/committees/

(e) the International Money Laundering Information Network (IMOLIN) - www.imolin.org

5.2 **Annual Report of the AMLCO**

5.2.1 **General**

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

The Annual Report is prepared and submitted for approval to the Board, within two (2) months from the end of each calendar year (the latest by the end of February). The Annual Report, after its approval by the Board, is submitted to CySEC together with the minutes of the meeting, during which the Annual Report has been discussed and approved. It is provided that the said minutes 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. These minutes and the Annual Report are submitted to CySEC within twenty (20) days from the date of the relevant meeting, and not later than three (3) months from the end of the calendar year.

5.2.2 **Content of the Annual Report**

The Annual Report deals with money laundering and terrorist financing preventive issues pertaining to the year under review and, as a minimum, covers the following:

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

(b) Information on the inspections and reviews performed by the AMLCO, reporting the material deficiencies and weaknesses identified in the policy, practices, measures, procedures and controls that the Company applies for the prevention of money laundering and terrorist financing. In this regard, 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 employees of the Company to the AMLCO according to paragraph 9(1)(e), and possible comments/observations thereon.

(d) The number of Reports submitted by the AMLCO to MOKAS, with information/details on the main reasons for suspicion and highlights of any particular trends.

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

(f) Summary figures, on an annualised basis, of clients' total cash deposits in Euro and other currencies in excess of the set limit of 10.000 Euro (together with comparative figures for the previous year) as

reported in the Monthly Prevention Statement. Any comments on material changes observed compared with the previous year are also reported.

(g) Information on the policy, measures, practices, procedures and controls applied by the Company in relation to high risk clients as well as the number and country of origin of high risk clients with whom a business relationship is established or an occasional transaction has been executed.

(h) Information on the systems and procedures applied by the Company for the ongoing monitoring of client accounts and transactions.

(i) Information on the measures taken for the compliance of branches and subsidiaries of the Company, that operate in countries outside the European Economic Area, with the requirements of the Directive in relation to client identification, due diligence and record keeping procedures and comments/information on the level of their compliance with the said requirements.

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

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

(l) Results of the assessment of the adequacy and effectiveness of staff training.

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

(n) Information on the structure and staffing of the department of the AMLCO as well as recommendations and timeframe for their implementation, for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against money laundering and terrorist financing.

5.3 **Monthly Prevention Statement**

The AMLCO prepares and submits to CySEC, on a monthly basis, the Form 144-08-11 which includes details for the total cash deposits accepted by the Company, the Internal Suspicions Reports, and the AMLCO's Reports to MOKAS.

The completion of the Form provides the opportunity to the Company initially to evaluate and, subsequently, to reinforce its systems of control and monitoring of its operations, for the purpose of early identification and detection of transactions in cash which may be unusual and/or carry enhanced risk of being involved in money laundering and terrorist financing operations. The said Form is completed and submitted to CySEC within fifteen (15) days from the end of each month.

5.4 **Application of appropriate measures and procedures on a Risk Based Approach**

The Company applies appropriate measures and procedures, on a risk based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be higher.

A risk-based approach:

(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 Company in a way that matches the risk of their particular business;

(c) allows the Board to apply its own approach in the formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics;

(d) helps to produce a more cost effective system; and

(e) promotes the prioritization of effort and actions of the Company in response to the likelihood of money laundering or terrorist financing occurring through the use of services provided by the Company.

A risk-based approach involves specific measures and procedures in assessing the most cost effective and proportionate way to manage the money laundering and terrorist financing risks faced by the Company.

Such measures and procedures are:

(a) identifying and assessing the money laundering and terrorist financing risks emanating from particular clients, financial instruments, services, and geographical areas of operation of the Company and its clients;

(b) documenting in this Manual, the policies, measures, procedures and controls to ensure their uniform application across the Company by persons specifically appointed for that purpose by the Board;

(c) managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls;

(d) continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

5.4.1 **Identification, recording and evaluation of risks**

5.4.1.1 **General**

The AMLCO has the responsibility to identify, record and evaluate all potential risks. The successful establishment of measures and procedures on a risk-based approach requires the clear communication of the measures and procedures that have been decided across the Company, along with robust mechanisms to ensure that these are implemented effectively, weaknesses are promptly identified and improvements are made wherever necessary.

A risk-based approach involves the identification, recording and evaluation of the risks that have to be managed. The Company assesses and evaluates the risk it faces, for usage of the services provided for the

purpose of money laundering or terrorist financing. The particular circumstances of the Company determine the suitable procedures and measures that need to be applied to counter and manage risk.

In the cases where the services and the financial instruments that the Company provides are relatively simple, involving relatively few clients, or clients with similar characteristics, then the Company applies procedures that focus on those clients who fall outside the 'norm'.

5.4.1.2 **Risk Factors**

The following risk factors are not exhaustive nor is there an expectation that the Company will consider all risk factors in all cases. The Company should take a holistic view of the risk associated with the situation and note that the presence of isolated risk factors does not necessarily move a relationship into a higher or lower risk category.

5.4.1.2.1 **Customer risk factors**

1. In relation to the customer's or a customer's beneficial owner's **business or professional activity**:
   - Does the customer or beneficial owner have links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the arms trade and defence, the extractive industries or public procurement?
   - Does the customer or beneficial owner have links to sectors that are associated with higher ML/TF risk, for example certain Money Service Businesses, casinos or dealers in precious metals?
   - Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?
   - Where the customer is a legal person or a legal arrangement, what is the purpose of their establishment? For example, what is the nature of their business?
   - Does the customer have political connections, for example, are they a Politically Exposed Person (PEP), or is their beneficial owner a PEP?
   - Does the customer or beneficial owner have any other relevant links to a PEP, for example are any of the customer's directors PEPs and, if so, do these PEPs exercise significant control over the customer or beneficial owner? Where a customer or their beneficial owner is a PEP, the Company must always apply enhanced due diligence measures.
   - Does the customer or beneficial owner hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain? For example, are they senior local or regional public officials with the ability to influence the awarding of public contracts, decision-making members of high-profile sporting bodies or individuals who are known to influence the government and other senior decision-makers?

- Is the customer a legal person subject to enforceable disclosure requirements that ensure that reliable information about the customer's beneficial owner is publicly available, for example public companies listed on stock exchanges that make such disclosure a condition for listing?
- Is the customer a credit or financial institution acting on its own account from a jurisdiction with an effective AML/CFT regime and is it supervised for compliance with local AML/CFT obligations? Is there evidence that the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML/CFT obligations or wider conduct requirements in recent years?
- Is the customer a public administration or enterprise from a jurisdiction with low levels of corruption?
- Is the customer's or the beneficial owner's background consistent with what the firm knows about their former, current or planned business activity, their business's turnover, the source of funds and the customer's or beneficial owner's source of wealth?

2. In relation to the customer's and the customer's beneficial owner's **reputation:**
   - Are there adverse media reports or other relevant sources of information about the customer, for example are there any allegations of criminality or terrorism against the customer or the beneficial owner? If so, are these reliable and credible? The Company should determine the credibility of allegations on the basis of the quality and independence of the source of the data and the persistence of reporting of these allegations, among other considerations. In this context, it is highlighted that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing.
   - Has the customer, beneficial owner or anyone publicly known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing? Does the firm have reasonable grounds to suspect that the customer or beneficial owner or anyone publicly known to be closely associated with them has, at some point in the past, been subject to such an asset freeze?
   - Does the firm know if the customer or beneficial owner has been the subject of a suspicious transactions report in the past?
   - Does the firm have any in-house information about the customer's or the beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship?
3. In relation to the customer's and the customer's beneficial owner's **nature and behaviour**:
   - Does the customer have legitimate reasons for being unable to provide robust evidence of their identity, perhaps because they are an asylum seeker?
   - Does the firm have any doubts about the veracity or accuracy of the customer's or beneficial owner's identity?

- Are there indications that the customer might seek to avoid the establishment of a business relationship? For example, does the customer look to carry out one transaction or several one-off transactions where the establishment of a business relationship might make more economic sense?
- Is the customer's ownership and control structure transparent and does it make sense? If the customer's ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?
- Does the customer issue bearer shares or does it have nominee shareholders?
- Is the customer a legal person or arrangement that could be used as an asset-holding vehicle?
- Is there a sound reason for changes in the customer's ownership and control structure?
- Does the customer request transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale? Are there grounds to suspect that the customer is trying to evade specific thresholds such as those set out in Article 11(b) of Directive (EU) 2015/849 and the Law where applicable?
- Does the customer request unnecessary or unreasonable levels of secrecy? For example, is the customer reluctant to share CDD information, or do they appear to want to disguise the true nature of their business?
- Can the customer's or beneficial owner's source of wealth or source of funds be easily explained, for example through their occupation, inheritance or investments? Is the explanation plausible?
- Does the customer use the products and services they have taken out as expected when the business relationship was first established?
- Where the customer is a non-resident, could their needs be better serviced elsewhere? Is there a sound economic and lawful rationale for the customer requesting the type of financial service sought?
- Is the customer a non-profit organisation whose activities could be abused for terrorist financing purposes?

5.4.1.2.2 **Countries and geographical areas**

When identifying the risk associated with countries and geographical areas, the Company should consider the risk related to below factors, taking into account that the nature and purpose of the business relationship will often determine the relative importance of individual country and geographical risk factors:

(a) the jurisdictions in which the customer and beneficial owner are based;

(b) the jurisdictions that are the customer's and beneficial owner's main places of business; and

(c) the jurisdictions to which the customer and beneficial owner have relevant personal links.

In particular:

- Where the funds used in the business relationship have been generated abroad, the level of predicate offences to money laundering and the effectiveness of a country's legal system will be particularly relevant.
- Where funds are received from, or sent to, jurisdictions where groups committing terrorist offences are known to be operating, firms should consider to what extent this could be expected to or might give rise to suspicion, based on what the firm knows about the purpose and nature of the business relationship.
- Where the customer is a credit or financial institution, the Company should pay particular attention to the adequacy of the country's AML/CFT regime and the effectiveness of AML/CFT supervision.
- Where the customer is a legal vehicle or trust, firms should take into account the extent to which the country in which the customer and, where applicable, the beneficial owner are registered effectively complies with international tax transparency standards.

Relevant factors in considering the **effectiveness of a jurisdiction's AML/CFT regime** include:

- Has the country been identified by the Commission as having strategic deficiencies in its AML/CFT regime, in line with Article 9 of the EU Directive? Where the Company deals with natural or legal persons resident or established in third countries that the Commission has identified as presenting a high ML/TF risk, the Company must always apply EDD measures.
- Is there information from more than one credible and reliable source about the quality of the jurisdiction's AML/CFT controls, including information about the quality and effectiveness of regulatory enforcement and oversight? Examples of possible sources include mutual evaluation reports by the Financial Action Task Force (FATF) or FATF-style Regional Bodies (FSRBs) (a good starting point is the executive summary and key findings and the assessment of compliance with Recommendations 10, 26 and 27 and Immediate Outcomes 3 and 4), the FATF's list of high-risk and noncooperative jurisdictions, International Monetary Fund (IMF) assessments and Financial Sector Assessment Programme (FSAP) reports.

It is hereby noted that membership of the FATF or an FSRB (e.g. MoneyVal) does not, of itself, mean that the jurisdiction's AML/CFT regime is adequate and effective. It is hereby noted that the EU Directive does not recognise the 'equivalence' of third countries and that EU Member States' lists of equivalent jurisdictions are no longer being maintained. To the extent permitted by national legislation, firms should be able to identify lower risk jurisdictions in line with the Risk Factors Guidelines issued by the European Supervisory Authorities (ESAs) and Annex II of the EU Directive.

Relevant risk factors when identifying the **level of terrorist financing risk associated with a jurisdiction** include:

- Is there information, for example from law enforcement or credible and reliable open media sources, suggesting that a jurisdiction provides funding or support for terrorist activities or that groups committing terrorist offences are known to be operating in the country or territory?
- Is the jurisdiction subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the United Nations or the European Union ?

Relevant risk factors when identifying a jurisdiction's **level of transparency and tax compliance** include:

- Is there information from more than one credible and reliable source that the country has been deemed compliant with international tax transparency and information sharing standards? Is there evidence that relevant rules are effectively implemented in practice? Examples of possible sources include reports by the Global Forum on Transparency and the Exchange of Information for Tax Purposes of the Organisation for Economic Co-operation and Development (OECD), which rate jurisdictions for tax transparency and information sharing purposes; assessments of the jurisdiction's commitment to automatic exchange of information based on the Common Reporting Standard; assessments of compliance with FATF Recommendations 9, 24 and 25 and Immediate Outcomes 2 and 5 by the FATF or FSRBs; and IMF assessments (e.g. IMF staff assessments of offshore financial centres).
- Has the jurisdiction committed to, and effectively implemented, the Common Reporting Standard on Automatic Exchange of Information, which the G20 adopted in 2014?
- Has the jurisdiction put in place reliable and accessible beneficial ownership registers?

Relevant risk factors when identifying the risk associated with **the level of predicate offences to money laundering** include:

- Is there information from credible and reliable public sources about the level of predicate offences to money laundering listed in Article 3(4) of the EU Directive, for example corruption, organised crime, tax crime and serious fraud? Examples include corruption perceptions indices; OECD country reports on the implementation of the OECD's anti-bribery convention; and the United Nations Office on Drugs and Crime World Drug Report.
- Is there information from more than one credible and reliable source about the capacity of the jurisdiction's investigative and judicial system effectively to investigate and prosecute these offences?

5.4.1.2.3 **Products, services and transactions risk factors**

The Company when identifying the risk associated with its products, services or transactions, it should consider the risk related to:

1. The **level of transparency**, or opaqueness, the product, service or transaction affords:
   - To what extent do products or services allow the customer or beneficial owner or beneficiary structures to remain anonymous, or facilitate hiding their identity? Examples of such products and

services include bearer shares, fiduciary deposits, offshore vehicles and certain trusts, and legal entities such as foundations that can be structured in such a way as to take advantage of anonymity and allow dealings with shell companies or companies with nominee shareholders.

- To what extent is it possible for a third party that is not part of the business relationship to give instructions, for example in the case of certain correspondent banking relationships?

2. the **complexity** of the product, service or transaction:
   - To what extent is the transaction complex and does it involve multiple parties or multiple jurisdictions, for example in the case of certain trade finance transactions?
   - To what extent do products or services allow payments from third parties or accept overpayments where this is would not normally be expected? Where third party payments are expected, does the firm know the third party's identity, for example is it a state benefit authority or a guarantor? Or are products and services funded exclusively by fund transfers from the customer's own account at another financial institution that is subject to AML/CFT standards and oversight that are comparable to those required under the EU Directive?
   - Does the Company understand the risks associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods?
3. the **value or size** of the product, service or transaction:
   - To what extent are products or services cash intensive, as are many payment services but also certain current accounts?
   - To what extent do products or services facilitate or encourage high-value transactions? Are there any caps on transaction values or levels of premium that could limit the use of the product or service for ML/TF purposes?

5.4.1.2.4 **Delivery channel risk factors**

When identifying the risk associated with the way in which the customer obtains the products or services they require, the Company should consider the risk related to:

(a) the extent to which the business relationship is conducted on a **non-face-to-face** basis:
   - Is the customer physically present for identification purposes? If they are not, has the firm used a reliable form of non-face-to-face CDD? Has it taken steps to prevent impersonation or identity fraud?
   - Has the customer been introduced by another part of the same financial group and, if so, to what extent can the firm rely on this introduction as reassurance that the customer will not expose the firm to excessive ML/TF risk? What has the firm done to satisfy itself that the group entity applies CDD measures to European Economic Area (EEA) standards in line with Article 28 of the EU Directive?

- Has the customer been introduced by a third party, for example a bank that is not part of the same group, and is the third party a financial institution or is its main business activity unrelated to financial service provision? What has the firm done to be satisfied that:
  (a) the third party applies CDD measures and keeps records to EEA standards and that it is supervised for compliance with comparable AML/CFT obligations in line with Article 26 of the EU Directive;
  (b) the third party will provide, immediately upon request, relevant copies of identification and verification data, inter alia in line with Article 27 of the EU Directive; and
  (c) the quality of the third party's CDD measures is such that it can be relied upon?
- Has the customer been introduced through a tied agent, that is, without direct firm contact? To what extent can the firm be satisfied that the agent has obtained enough information so that the firm knows its customer and the level of risk associated with the business relationship?
- If independent or tied agents are used, to what extent are they involved on an ongoing basis in the conduct of business? How does this affect the firm's knowledge of the customer and ongoing risk management?

(b) any **introducers or intermediaries** the firm might use and the nature of their relationship with the firm:

- Are they a regulated person subject to AML obligations that are consistent with those of the EU Directive?
- Are they subject to effective AML supervision? Are there any indications that the intermediary's level of compliance with applicable AML legislation or regulation is inadequate, for example has the intermediary been sanctioned for breaches of AML/CFT obligations?
- Are they based in a jurisdiction associated with higher ML/TF risk? Where a third party is based in a high-risk third country that the Commission has identified as having strategic deficiencies, firms must not rely on that intermediary. However, to the extent permitted by national legislation, reliance may be possible provided that the intermediary is a branch or majority-owned subsidiary of another firm established in the Union, and the firm is confident that the intermediary fully complies with group-wide policies and procedures in line with Article 45 of the EU Directive.

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

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

- adaptation of the Client Due Diligence Procedures in respect of clients in line with their assessed Money Laundering and Terrorist Financing risk;
- requiring the quality and extent of required identification data for each type of client to be of a certain standard (e.g. documents from independent and reliable sources, third person information, documentary evidence);
- obtaining additional data and information from the clients, where this is appropriate for the proper and complete understanding of their activities and source of wealth and for the effective management of any increased risk emanating from the particular Business Relationship or the Occasional Transaction;
- ongoing monitoring of high risk clients' transactions and activities, as and when applicable.

In this respect, it is the duty of the AMLCO to develop and constantly monitor and adjust the Company's policies and procedures with respect to the Client Acceptance Policy and client due diligence and identification procedures, 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 Report, as applicable.

5.5 **Ongoing monitoring of accounts and transactions**

The Company has a full understanding of normal and reasonable account activity of their customers as well as of their economic profile and have 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.

The procedures and intensity of monitoring accounts and 1examining transactions are based on the level of risk and, as a minimum, achieve the following:

(a) identifying all high risk customers. Therefore, the systems or the measures and procedures of the Company are able to produce detailed lists of high risk customers so as to facilitate enhanced monitoring of accounts and transactions;

(b) detecting of unusual or suspicious transactions that are inconsistent with the economic profile of the customer for the purposes of further investigation;

(c) the investigation of unusual or suspicious transactions from the employees who have been appointed for that purpose; the results of the investigations are recorded in a separate memo and kept in the file of the customer concerned;

(d) all necessary measures and actions must be taken, based on the investigation findings of point (c), including any internal reporting of suspicious transactions/activities to the AMLCO,

(e) ascertaining the source and origin of the funds credited to accounts.

The monitoring of accounts and transactions are carried out in relation to specific types of transactions and 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 customers who do not have a contact with the Company as well as dormant accounts exhibiting unexpected movements.

6 CLIENT DUE DILIGENCE AND IDENTIFICATION PROCEDURES

6.1 When to apply CDD and identification procedures

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

(a) when establishing a Business Relationship

(b) when carrying out Occasional Transactions amounting to Euro 15,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(c) when there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction;

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

6.2 Ways of applying CDD and identification procedures

The identification procedures and the customer due diligence measures, include the following:

(i) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

(ii) identifying the beneficial owner's identity and taking reasonable measures to verify that person's identity so that the Company is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer;

(iii) assessing and, depending on the case, obtaining information on the purpose and intended nature of the business relationship;

(iv) Conducting ongoing 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 Company in relation to the customer, the business and risk profile of the customer, including where necessary, relating to the source of funds and ensuring that the documents, data or information held are kept up-to-date;

Provided that, in the application of the measures referred to in paragraphs (i) and (ii), the Company shall also verify that any third person purporting to act on behalf of the customer is duly authorised by the customer for this purpose and identifies and verifies the identity of that person.

The obliged entities apply each of the customer due diligence measures and identification procedures set out in paragraph (2) above but may determine the extent of such measures on a risk-sensitive basis taking into account at least the following variables:

(A) the purpose of an account or relationship;

(B) the level of assets to be deposited by a customer or the size of transactions undertaken;

(C) the regularity or duration of the business relationship.

The obliged entities must be able to demonstrate to CySEC that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing they are exposed to.

6.3 **Proof of identity**

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

(a) It is reasonable possible to establish that the customer is the person he claims to be; and

(b) The person who examines the customer's evidence is satisfied, in accordance with the procedures followed under this Manual, that the customer is actually the person he claims to be.

6.4 **Simplified customer due diligence**

The Company may apply simplified customer due diligence measures, so long as it has previously ensured that the business relationship or the transaction presents a lower degree of risk and provided that the Company carries out sufficient monitoring of the transactions and the business relationships to enable the detection of unusual or suspicious transactions.

When assessing the risks of money laundering or terrorist financing which relate to types of customers, geographical areas and particular products, services, transactions or delivery channels, the Company takes into account at least the factors of potentially lower risk situations set out in Appendix E.

6.5 **Enhanced customer due diligence**

The Company applies enhanced customer due diligence measures, in addition to the measures referred to in section 6.2.:

(a) When it is transacting with a natural person or legal entity with an establishment in a high-risk third country - provided that, enhanced customer due diligence measures need not be automatically invoked with respect to branches or majority owned subsidiaries of the obliged entity established in the European Union which are located in high-risk third countries, where those branches or majority owned subsidiaries fully comply with the group-wide policies and procedures in accordance with the Law and, in such a case, the Company uses the risk-based approach;

(b) In cross border correspondent relationships with a third-country respondent institution, the Company

i. gathers sufficient information about the respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision;

ii. assesses the respondent institution's prevention of money laundering and terrorist financing controls.

iii. obtains approval from senior management before establishing new correspondent relationships;

iv. documents the respective responsibilities of each institution;

v. with respect to payable-through accounts, be satisfied that the respondent institution has verified the identity of, and performed ongoing due diligence on, the customers having direct access to accounts of the correspondent institution, and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request.

(c) In transactions or business relationships with a politically exposed person (PEP), the Company:

i. has in place appropriate risk management systems, including risk based procedures, to determine whether the customer or the beneficial owner of the customer is a politically exposed person.

ii. applies the following measures in cases of business relationships with a politically exposed person:

- Receives approval from senior management for establishing or continuing a business relationship with such a person;
- takes adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such a person;
- conducts enhanced, ongoing monitoring of that business relationship:

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

iii. applies the measures referred to in sub-paragraphs (i) and (ii) to family members or to the persons which are known to be close associates of a politically exposed person.

The Company applies enhanced customer due diligence measures, 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 Company takes into account at least the factors of potentially higher risk situations, as set out in Appendix F.

The Company 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.

6.6 **Construction of an economic profile**

1. The Company is satisfied that it's dealing with a real person and, for this reason, obtains sufficient evidence of identity to verify that the person is who he claims to be. Furthermore, the Company verifies the identity of the beneficial owners of the customers' accounts. In the cases of legal persons, the Company obtains adequate data and information so as to understand the ownership and control structure of the customer. Irrespective of the customer's type (e.g. natural or legal person, sole trader or partnership), the Company requests and obtains sufficient data and information regarding the customer's business activities and the expected pattern and level of transactions. However, it is noted that no single form of identification can be fully guaranteed as genuine or representing correct identity and, consequently, the identification process will generally need to be cumulative.
2. The verification of the customers' identification is 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.
3. A person's residential and business address is an essential part of his identity and, thus, a separate procedure for its verification, according to Appendix G is followed.
4. It is never acceptable to use the same verification data or information for verifying the customer's identity and verifying its home address. (5)
5. The data and information that are collected before the establishment of the business relationship, with the aim of constructing the customer's economic profile and, as a minimum, include the following :
   (a) the purpose and the reason for requesting the establishment of a business relationship;
   (b) 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;
   (c) the customer's size of wealth and annual income and the clear description of the main business/professional activities/operations.
6. The data and information that are used for the construction of the customer's-legal person's economic profile include, inter alia, the name of the company, the country of its incorporation, the head offices address, the names and the identification information of the beneficial owners, directors and authorised signatories, financial information, ownership structure of the group that the company may be a part of (country of incorporation of the parent company, subsidiary companies and associate companies, main activities and financial information). The said data and information are recorded in a separate form designed for this purpose which is retained in the customer's file along with all other

documents as well as all internal records of meetings with the respective customer. The said form is updated regularly or whenever new information emerges that needs to be added to the economic profile of the customer or alters existing information that makes up the economic profile of the customer. Identical data and information with the abovementioned are obtained in the case of a customer-natural person, and in general, the same procedures with the abovementioned are followed.

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

7 BACK OFFICE OBLIGATIONS – RECORD KEEPING/UPDATING OF DOCUMENTATION

7.1 General

The Back Office Department is responsible for the record keeping and updating of the documents/data mentioned in this Manual. The documents/data, are 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 relevant to ongoing investigations are kept until MOKAS confirms that the investigation has been completed and the case has been closed.

The documentation is updated in the following frequency:

1. For high risk clients: annually
2. For medium and low risk clients: every two (2) years

If clients denies or omits to provide updated documentation within 30 days' of such request then the Back Office Department informs the AMLCO accordingly.

7.2 Format of records

The retention of the documents/data, other than the original documents or their certified true copies that are kept in a hard copy form, may be in other forms, such as electronic form, provided that the Company is able to retrieve the relevant documents/data without undue delay and present them at any time, to CySEC or to MOKAS, after a request.

7.3 Certification and language of documents

(1) The documents/data obtained, for compliance with the Directive, are in their original form or in a certified true copy form. In the case that the documents/data are certified as true copies by a different

person than the Company itself or by the third person, the documents/data must be apostilled or notarised.

(2) The documentation must be translated in Greek or English when the original is in any other language.

8 EMPLOYEES' OBLIGATIONS

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

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

(3) According to section 26 of the Law, the Company's employees fulfill their legal obligation to report their suspicions regarding money laundering and terrorist financing, after their compliance with subparagraph (2).

9 APPENDIX A – EXAMPLES OF SUSPICIOUS TRANSACTIONS

9.1 **Money Laundering**

1. Transactions with no discernible purpose or are unnecessarily complex.
2. Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the customer.
3. The transactions or the size of the transactions requested by the customer do not comply with his usual practice and business activity.
4. Large volume of transactions and/or money deposited or credited into, an account when the nature of the customer's business activities would not appear to justify such activity.
5. The business relationship involves only one transaction or it has a short duration.
6. There is no visible justification for a customer using the services of the Company. For example the customer is situated far away from the Company and in a place where he could be provided services by another firm.
7. There are frequent transactions in the same financial instrument without obvious reason and in conditions that appear unusual (churning).
8. Any transaction the nature, size or frequency appear to be unusual, e.g. cancellation of an order, particularly after the deposit of the consideration.
9. 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.
10. Settlement of the transaction by a third person which is different than the customer which gave the order.
11. Instructions of payment to a third person that does not seem to be related with the instructor.
12. 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.
13. A customer is reluctant to provide complete information when establishes a business relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with financial organisations, names of its officers and directors, or information on its business location. The customer usually provides minimum or misleading information that is difficult or expensive for the Company to verify.
14. A customer provides unusual or suspicious identification documents that cannot be readily verified.
15. A customer's home/business telephone is disconnected.
16. A customer that makes frequent or large transactions and has no record of past or present employment experience.

17. Difficulties or delays on the submission of the financial statements or other identification documents, of a customer/legal person.
18. A customer who has been introduced by a foreign company, 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.
19. The stated occupation of the customer is not commensurate with the level or size of the executed transactions.
20. Unexplained inconsistencies arising during the process of identifying and verifying the customer (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).
21. Complex trust or nominee network.
22. Transactions or company structures established or working with an unneeded commercial way. e.g. companies with bearer shares or bearer financial instruments or use of a postal box.
23. Changes in the lifestyle of employees of the Company, e.g. luxurious way of life or avoiding being out of office due to holidays.
24. Changes the performance and the behaviour of the employees of the Company.

9.2 **Terrorist Financing**

1. Sources and methods

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

Legal fund raising methods used by terrorist groups include:

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

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

2. Non-profit organisations

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

i. Establishing a non-profit organisation with a specific charitable purpose but which actually exists only to channel funds to a terrorist organisation.

ii. A non-profit organisation with a legitimate humanitarian or charitable purpose is infiltrated by terrorists who divert funds collected for an ostensibly legitimate charitable purpose for the support of a terrorist group.

iii. The non-profit organisation serves as an intermediary or cover for the movement of funds on an international basis.

iv. The non-profit organisation provides administrative support to the terrorist movement.

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

(a) Inconsistencies between the apparent sources and amount of funds raised or moved.

(b) A mismatch between the type and size of financial transactions and the stated purpose and activity of the non-profit organisation.

(c) A sudden increase in the frequency and amounts of financial transactions for the account of a non-profit organisation.

(d) Large and unexplained cash transactions by non-profit organisations.

(e) The absence of contributions from donors located within the country of origin of the non-profit organisation.

10 APPENDIX B – INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING	
INFORMER'S DETAILS	
Name:	
Department:	
Position:	
Tel:	
E-mail:	
CLIENT DETAILS	
Name:	
Passport/ID no,:	
Date of Birth:	
Nationality	
Place of residence	
Occupation:	
Account no.:	
INFORMATION/SUSPICION	
Brief description of activities/transaction:	
Reason(s) for suspicion:	
Informer's Signature:	
Date:	
FOR AMLCO'S USE	
Date Received:	
Time Received:	
Ref.:	
Reported to MOKAS:	Yes/No
Date Reported:	
Ref	

11 APPENDIX C – INTERNAL EVALUATION REPORT

INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING	
Reference:	
Customer's Details:	
Informer:	
Department:	
INQUIRIES UNDERTAKEN (Brief Description)	
ATTACHED DOCUMENTS	
AMLCO'S DECISION	
FILE NUMBER:	
AMLCO's signature:	……..
Date:	

12 APPENDIX D - AMLCO'S REPORT TO THE UNIT FOR COMBATING MONEY LAUNDERING ('MOKAS')

AMLCO'S REPORT TO THE UNIT FOR COMBATING MONEY LAUNDERING ('MOKAS')		
I. GENERAL INFORMATION		
Financial Organisation's Name:		
Address where customer's account is kept:		
Date when a business relationship established or occasional transaction was carried out:		
Type of account(s) and number(s):		
II. DETAILS OF NATURAL PERSON(S) AND/OR LEGAL ENTITY(IES) INVOLVED IN THE SUSPICIOUS TRANSACTION(S)		
(A) NATURAL PERSONS		
	Beneficial owner(s) of the account(s)	Authorised signatory(ies) of the account(s)
Name(s):		
Residential address(es):		
Business address(es):		
Occupation and Employer:		
Date and place of birth:		
Nationality and passport number		
(B) LEGAL ENTITIES		
Legal entity's name, country and date of incorporation:		
Business address:		
Main activities:		

13 APPENDIX E - LIST OF FACTORS AND TYPES OF EVIDENCE OF POTENTIALLY LOWER RISK OF ML/TF

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 paragraph (3);

2. **Product, service, transaction or delivery channel risk factors:**
   (a) 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;
   (b) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership such as certain types of electronic money;

3. **Geographical risk factors:**
   (a) Member States;
   (b) third countries having effective AML/CFT systems;
   (c) third countries identified by credible sources as having a low level of corruption or other criminal activity;
   (d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

14 APPENDIX F - 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 paragraph (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 company appears unusual or excessively complex given the nature of the company's business;
2. **Product, service, transaction or delivery channel risk factors:**
   (a) private banking;
   (b) products or transactions that might favour anonymity;
   (c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;
   (d) payment received from unknown or 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) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
   (b) countries identified by credible sources as having significant levels of corruption or other criminal activity;
   (c) countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;
   (d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

15 APPENDIX G - SPECIFIC CUSTOMER IDENTIFICATION ISSUES

1. **Natural persons residing in the Republic**

(a) The Company ascertain the true identity of natural persons who are residents of the Republic of Cyprus by obtaining the following information:

i. true name and/or names used as these are sated on the official identity card or passport,

ii. full permanent address in the Republic, including postal code,

iii. telephone (home and mobile) and fax numbers,

iv. e-mail address , if any,

v. date and place of birth,

vi. nationality and

vii. details of the profession and other occupations of the customer including the name of employer/business organisation.

(b) The acceptable method for the verification of the identification of a customer's identity is the reference to an original document which is issued by an independent and reliable source that carries the customer's photo. After the Company is satisfied for the customer's identity from the original identification documents presented, it keeps copies of the pages containing all relevant information which are certified, by the Company, as true copies of the original documents.

(c) In addition to the name verification, it is important that the customer's permanent address is also verified by using one of the following ways:

i. visit at the place of residence (in such a case, the Company's officer who carries out the visit prepares a memo which is retained in the customer's file), and

ii. 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 (to protect against forged or counterfeit documents, the prospective customers are required to produce original documents).

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

2. **Natural persons not residing in the Republic**

(a) For customers who are not normally residing in the Republic, in addition to the information collected according to point (1) of the present Appendix, the Company, without prejudice to the application on a risk-sensitive basis, requires and receives information on public positions which

the prospective customer holds or held in the last twelve months as well as whether he is a close relative or associate of such individual, in order to verify if the customer is a politically exposed person, according to point (5) of the Fourth Appendix.

(b) For those customers not residing in the Republic, passports are always requested and, if available, official national identity cards issued by competent authorities of their country of origin are obtained and certified true copies of the pages containing the relevant information from the said documents are obtained and kept in the customers' files. In addition, it is advised, if in doubt for the genuineness of any document (passport, national identity card or documentary evidence of address), to seek verification of identity with an Embassy or the Consulate of the issuing country or a reputable credit or financial institution situated in the customer's country of residence.

(c) 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 regard, passport's number, issuing date and country as well as the customer's date of birth always appear on the copies of documents obtained, so that the Company would be in a position to verify precisely whether a customer 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.

3. 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 points (1) and (2) of the present Appendix.

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

In the case of accounts in the name of unions, societies, provident funds and charities, the Company ascertains their purpose of operation and verifies their legitimacy by requesting the production of the articles and memorandum of association/procedure rules and registration documents with the competent governmental authorities (in case the law requires such registration). Furthermore, the Company obtains 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 points (1) and (2) of the present Appendix.

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

(a) 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 is verified according to the procedures set in points (1) and (2) of the present

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

(b) The Company obtains documentary evidence of the head office address of the business, ascertains the nature and size of its activities and receives all the information required according to section 6.6 for the creation of the economic profile of the business.

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

6. <u>Accounts of legal persons</u>

(a) for customers that are legal persons, it is established 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 points (1) and (2) of the present Appendix.

(b) The Company takes 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.

(c) 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:

i. the registered number,

ii. the registered corporate name and trading name used,

iii. the full addresses of the registered office and the head offices,

iv. the telephone numbers, fax numbers and e-mail address,

v. the members of the board of directors,

vi. the individuals that are duly authorised to operate the account and to act on behalf of the legal person,

vii. the beneficial owners of private companies and public companies that are not listed in a regulated market of a European Economic Area country or a third country with equivalent disclosure and transparency requirements,

viii. the registered shareholders that act as nominees of the beneficial owners,

ix. The economic profile of the legal person, according to the provisions of section 6.6.

(d) For the verification of the identity of the legal person, the Company requests and obtains, inter alias, original or certified true copies of the following documents:

i. certificate of incorporation and certificate of good standing of the legal person,

ii. certificate of registered office,

iii. certificate of directors and secretary,

iv. certificate of registered shareholders in the case of private companies and public companies that are not listed in a regulated market of a European Economic Area country or a third country with equivalent disclosure and transparency requirements,

v. memorandum and articles of association of the legal person,

vi. a resolution of the board of directors of the legal person for the opening of the account and granting authority to those who will operate it,

vii. 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,

viii. documents and data for the verification, according to the provisions of the present Manual, 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.

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

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

(g) As an additional due diligence measure, on a risk-sensitive basis, the Company may carry out a search and obtain information from the records of the Registrar of Companies and Official Receiver of the Republic (for domestic companies) or from a corresponding authority in the company's (legal person's) country of incorporation (for foreign companies) and/or request information from other sources in order to establish that the applicant company (legal person) is not, nor is in the process of being dissolved or liquidated or struck off from the registry of the Registrar of Companies and Official Receiver and that it continues to be registered as an operating company in the records of the Registrar of Companies and Official Receiver of the Republic or by an appropriate authority outside the Republic. It is pointed out that, if at any later stage any changes occur in the structure or the ownership status or to any details of the legal person, or any suspicions arise emanating from changes in the nature of the transactions performed by the legal person via its account, then it is imperative that further enquiries should be made for ascertaining the consequences of these changes on the documentation and information held by the Company for the legal person and all additional documentation and information for updating the economic profile of the legal person is collected.

(h) In the case of a customer-legal person that requests the establishment of a business relationship or the execution of an occasional transaction and whose direct/immediate and principal shareholder is another legal person, registered in the Republic or abroad, the Company, before establishes a business relationship or executes an occasional transaction, verifies the ownership structure and the identity of the natural persons who are the beneficial owners and/or control the other legal person.

(i) Apart from verifying the identity of the beneficial owners, the Law requires that the persons who have the ultimate control over the legal person's business and assets are identified. In the cases that the ultimate control rests with the persons who have the power to manage the funds, accounts or investments of the legal person without requiring authorisation and who would be in a position to override the internal procedures of the legal person, the Company, verifies 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.

(j) In cases where the beneficial owner of a legal person, requesting the establishment of a business relationship or the execution of an occasional transaction, is a trust set up in the Republic or abroad, the Company implements the procedure provided in Appendix H.

7. <u>Investment funds, mutual funds and firms providing financial or investment services</u>

(a) the Company may 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 European Economic Area or a third country which according to a decision of the Advisory Authority for Combating Money Laundering Offences and Terrorist Financing it has been determined that applies requirements equivalent to those laid down in the European Union Directive, provided that:

i. the said persons 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

ii. are subject to supervision for the prevention of money laundering and terrorist financing purposes.

(b) 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 (a) above, the Company requests and obtains, in addition to the abovementioned, in previous points, documentation and the information required by the Directive for the identification and verification of persons, including the beneficial owners, the following:

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

ii. 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 customer.

(c) In the case of investment funds and mutual funds the Company, apart from identifying beneficial owners, obtains 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.

8. <u>Nominees or agents of third persons</u>

(a) The Company takes reasonable measures to obtain adequate documents, data or information for the purpose of establishing and verifying the identity, according to the procedures set in the previous points of the present Appendix:

i. the nominee or the agent of the third person, and

ii. any third person on whose behalf the nominee or the agent is acting.

(b) In addition, the Company obtains a copy of the authorisation agreement that has been concluded between the interested parties.

16 APPENDIX H – HIGH RISK CUSTOMERS

1. Non face to face customers

(a) Whenever a customer requests the establishment of a business relationship or an occasional transaction, a personal interview is recommended during which all information for customer identification should be obtained. In situations where a customer, especially a non-resident of the Republic, requests the establishment of a business relationship or an occasional transaction by mail, telephone or through the internet without presenting himself for a personal interview, the Company shall follow the established customer identification and due diligence procedures, as applied for customers with whom it comes in direct and personal contact and obtain the same exact identification information and documents as required by the Law and Directive, depending on the type of the customer. The said identification information and documents kept by the Financial Organization in its records shall take the following form:

i. Original, or

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

iii. True copy of the original, where the certification is made by third parties, in cases where they establish the customer's identity, pursuant to Article 67 of the Law and the provisions of paragraph 25 of the Directive, or

iv. True copy of the original, where the certification is made by a competent authority or person that, pursuant to the relevant provisions of the laws of their country, is responsible to certify the authenticity of documents or information, or

v. Provided that at least one of the procedures referred to in paragraph (b) below is followed:

(i) Copy of the original, or

(ii) Data and information collected via electronic verification in accordance with the provisions of paragraph (c) below.

(b) Instead of the measure provided for in Article 64(1)(a)(ii) of the Law, other practical procedures, which may be adopted for the implementation of the measure of Article 64(1)(a)(i) of the Law with regard to customers with whom the Financial Organization does not come to immediate and personal contact, are as follows:

i. The first payment of the operations is carried out through an account opened in the customer's name with a credit institution operating and licensed in a third country, which, according to the Advisory Authority's decision, imposes requirements on combating money laundering equivalent to those of the EU Directive.

ii. A direct confirmation of the establishment of a business relationship is obtained through direct personal contact, as well as, the true name, address and passport/identity card number of the customer, from a credit institution or a financial institution with which the customer cooperates, operating in a Member State or in a Third Country, which, according to the Advisory Authority's decision, imposes requirements on combating money laundering equivalent to those of the EU Directive (or a true copy of the confirmation).

iii. Telephone contact with the customer at his home or office, on a telephone number which has been verified from independent and reliable sources. During the telephone contact, the Financial Organization shall confirm additional aspects of the identity information submitted by the customer during the procedure of opening his account.

iv. Communication via video call with the customer, provided the video recording and screen shot safeguards apply to the communication. It is provided that a customer, whose identity was verified hereunder cannot deposit an amount over €2.000 per annum, irrespective of the number of accounts that he keeps with the Financial Organization, unless an additional measure of paragraph (b) of the present or of article 64(1)(a)(ii) of the Law is taken in order to verify his identity. During the internet communication, the Financial Organization shall confirm additional aspects of the identity details submitted by the customer when opening his account.

It is provided that the Financial Organization shall apply appropriate measures and procedures in order to:

1. confirm and monitor both the amount of the customer's deposit and the risk for money laundering or terrorist financing and take additional measures to verify the customer's identity depending on the degree of the risk,
2. ensure the normal conduct of business is not interrupted where the amount of the deposit exceeds the amount of €2.000 per annum;
3. warn the customer appropriately and in due time for the above procedure in order to obtain the customer's express consent prior to its commencement.
4. Communication with the customer through at an address that the Financial Organization has previously verified from independent and reliable sources, in the form of a registered letter (For example, such communication may take the form of a direct mailing of account opening documentation to him, which the customer shall return to the Financial Organization or the Company may send security codes required by the customer to access the accounts opened through the internet).

(c) Performing an electronic verification:

i. Electronic identity verification is carried out either directly by the Financial Organization or through a third party. Both the Financial Organization and the said third parties cumulatively satisfy the following conditions:

i. the electronic databases kept by the third party or to which the third party or the Financial Organization has access are registered to and/or approved by the Data Protection Commissioner in order to safeguard personal data (or the corresponding competent authority in the country the said databases are kept).

ii. electronic databases provide access to information referred to both present and past situations showing that the person really exists and providing both positive information (at least the customer's full name, address and date of birth) and negative information (e.g. committing of offences such as identity theft, inclusion in deceased persons records, inclusion in sanctions and restrictive measures' list by the Council of the European Union and the UN Security Council).

iii. electronic databases include a wide range of sources with information from different time periods with real-time update and trigger alerts when important data alter.

iv. transparent procedures have been established allowing the Financial Organization to know which information was searched, the result of such search and its significance in relation to the level of assurance as to the customer's identity verification.

v. procedures have been established allowing the Financial Organization to record and save the information used and the result in relation to identity verification.

2. Information must come from two or more sources. The electronic verification procedure shall at least satisfy the following correlation standard:

(a) identification of the customer's full name and current address from one source, and

(b) identification of the customer's full name and either his current address or date of birth from a second source.

3. For purposes of carrying out the electronic verification, the Financial Organization shall establish procedures in order to satisfy the completeness, validity and reliability of the information to which it has access. It is provided that the verification procedure shall include a search of both positive and negative information.

(d) It is provided that the Financial Organization evaluates the results in order the conditions of Article 61(3) of the Law to be satisfied. The Financial Organization establishes mechanisms for the carrying out of quality controls in order to assess the quality of the information on which it intends to rely.

(e) The requirements of Article 64(1)(a) of the Law and of this Directive shall also apply to companies or other legal persons requesting to establish a business relationship or an occasional transaction by mail, telephone or through the internet. The Financial Organization shall take additional

measures to ensure that the companies or other legal persons operate from the address of their main offices and carry out legitimate activities in all respects.

2. **Accounts in the names of companies whose shares are in bearer form**

The Company may accept a request for the establishment of a business relationship or for an occasional transaction from companies whose own shares or those of their parent companies (if any) have been issued in bearer form by applying, in addition to the procedures of paragraph 6 of Appendix G, all the following supplementary due diligence measures:

(a) 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 European Economic Area that it has under its own custody the bearer share certificates and, in case of transferring their ownership to another person, shall inform the Company accordingly.

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

(c) If the opening of the account has been recommended by a third person, at least once every year, the third person who has introduced the customer provides a written confirmation that the capital base and the shareholding structure of the company or that of its holding company (if any) has not been altered by the issue of new bearer shares or the cancellation of existing ones. If the account has been opened directly by the company, then the written confirmation is provided by the company's directors.

(d) When there is a change to the beneficial owners, the Company examines whether or not to permit the continuance of the account's operation.

3. **Trusts accounts**

(a) Without prejudice of the provisions of section 65(2) of the Law, when the Company establishes a business relationship or carries out an occasional transaction with trusts, it must 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 customer identification procedures prescribed in the Law and the Directive.

(b) Furthermore, the Company ascertains 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 customer's file.

4. **'Client accounts' in the name of a third person**

(a) A Company may open "client accounts" (e.g. omnibus accounts) in the name of financial institutions from European Economic Area countries or a third country which, in accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing it has been determined that it applies procedures and measures for preventing money laundering and terrorist financing equivalent to the requirements of the European Union Directive. In these cases the Company ascertains the identity of the abovementioned financial institutions according to the customer identification procedures prescribed in the Law and the Directive.

(b) In the case that the opening of a "client account" is requested by a third person acting as an auditor/accountant or an independent legal professional or a trust and company service provider situated in a country of the European Economic Area or a third country which, in accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing has been determined that it applies procedures and measures for preventing money laundering and terrorist financing equivalent to the requirements of the European Union Directive, the Company may proceed with the opening of the account provided that the following conditions are met:

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

ii. 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.

iii. The AMLCO has assessed the customer identification and due diligence procedures implemented by the third person and has found them to be in line with the Law and this Directive. A record of the assessment should be prepared and kept in a separate file maintained for each third person.

iv. The third person make available to the Company obtains all the data and documents prescribed in section 67(3) of the Law.

5. <u>Politically exposed persons' accounts</u>

(a) The establishment of a business relationship or the execution of an occasional transaction with politically exposed persons as interpreted in Article 2(1) of the Law, may expose a Company to enhanced risks, especially, if the potential customer seeking to establish a business relationship or the execution of an occasional transaction is a politically exposed person, a member of his immediate family or a close associate that is known to be associated with a politically exposed person. The Company should 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.

(b) In order to effectively manage such risks, the Company assess the countries of origin of their customers 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 Financial Action Task Force, according to point 7 of this Appendix. 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 Company may 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.

(c) The meaning 'politically exposed persons' includes the following natural persons who are or have been entrusted with prominent public functions' in a foreign country:

i. heads of State, heads of government, ministers and deputy or assistant ministers,

ii. members of parliaments,

iii. 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,

iv. members of courts of auditors or of the boards of central banks,

v. ambassadors, chargıs d'affaires and high-ranking officers in the armed forces, vi. members of the administrative, management or supervisory bodies of Stateowned enterprises.

(d) Without prejudice to the application, on a risk-sensitive basis, of enhanced customer due diligence measures, where a person has ceased to be entrusted with a prominent public function within the meaning of point 5(c) of this Appendix for a period of at least one year, the Company shall not be obliged to consider such a person as politically exposed.

(e) None of the categories set out in point 5(c) of this Appendix shall be understood as covering middle ranking or more junior officials. 'Immediate family members' includes the following:

i. the spouse or the person with which cohabit for at least one year,

ii. the children and their spouses or the persons with which cohabit for at least one year,

iii. the parents.

(f) 'Persons known to be close associates' includes the following:

i. 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 5(c) of this Appendix,

ii. 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 5(c) of this Appendix.

(g) Without prejudice to the provisions of section 64(1)(c) of the Law, the Company adopts the following additional due diligence measures when it establishes a business relationship or carry out an occasional transaction with a politically exposed person:

i. Put in place appropriate risk management procedures to enable it to determine whether a prospective customer is a politically exposed person. Such procedures may include, depending on the degree of risk, the acquisition and installation of a reliable commercial electronic database for politically exposed persons, seeking and obtaining information from the customer himself or from publicly available information. In the case of legal entities and arrangements, the procedures aim at verifying whether the beneficial owners, authorised signatories and persons authorised to act on behalf of the legal entities and arrangements constitute politically exposed persons. In case of identifying one of the above as a politically exposed person, then automatically the account of the legal entity or arrangement should be subject to the relevant procedures specified in the Law and the Directive.

ii. The decision for establishing a business relationship or the execution of an occasional transaction with a politically exposed person is taken by an executive director of the Company and the decision is then forwarded to the AMLCO. When establishing a business relationship with a customer (natural or legal person) and subsequently it is ascertained that the persons involved are or have become politically exposed persons, then an approval is given for continuing the operation of the business relationship by an executive director of the Company which is then forwarded to the AMLCO.

iii. Before establishing a business relationship or executing an occasional transaction with a politically exposed person, the Company obtains adequate documentation to ascertain not only the identity of he said person but also to assess his business reputation (e.g. reference letters from third parties).

iv. The Company creates the economic profile of the customer by obtaining the information specified in section 6.6. The details of the expected business and nature of activities of the customer forms the basis for the future monitoring of the account. The profile should be regularly reviewed and updated with new data and information. The Company is particularly cautious and most vigilant where its customers are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks.

v. The account is subject to annual review in order to determine whether to allow its continuance of operation. A short report is prepared summarising the results of the review by the person who is in charge of monitoring the account. The report is submitted for consideration and approval to the Board and filed in the customer's personal file.

6. <u>Electronic gambling/gaming through the internet</u>

(a) The Company may establish a business relationship or execute an occasional transaction in the names of persons who are involved in the abovementioned activities provided that these persons are licensed by a competent authority of a country of the European Economic Area or a third country which, in accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing it has been determined that it applies procedures equivalent to the requirements of the EU Directive. For this purpose, the Company requests and obtains, apart from the data and information required by the Directive, copy of the licence that has been granted to the said persons by the competent supervisory/regulatory authority, the authenticity of which must be verified either directly with the supervisory/regulatory authority or from other independent and reliable sources.

(b) Furthermore, the Company collects adequate information so as to understand the customers' control structure and ensures that the said customers apply adequate and appropriate systems and procedures for customer identification and due diligence for the prevention of money laundering and terrorist financing.

(c) In the case that the customer is a person who offers services (e.g. payment providers, software houses, card acquirers) to the persons mentioned in point 6(a) of the present Appendix, then the Company requests and obtains, apart from the data and information required by the Directive, adequate information so as to be satisfied that the services are offered only to licensed persons. Also, it obtains information necessary to completely understand the ownership structure and the group in which the customer belongs, as well as any other information that is deemed necessary so as to establish the customer's economic profile. Additionally, the Company obtains the signed agreement between its customer and the company that is duly licensed for electronic gambling/gaming activities through the internet, by a competent authority of a country mentioned in point 6(a) of the present Appendix,

(d) For all the above cases, the decision for the establishment of a business relationship or the execution of an occasional transaction is taken by an executive director of the Company and the decision is then forwarded to the AMLCO. Moreover, the account of the said customer 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 is prepared and submitted for consideration and approval to the Board and filed in the customer's personal file.

7. <u>Customers from countries which inadequately apply Financial Action Task Force's recommendations</u>

(a) The Financial Action Task Force's ("FATF") 40+9 Recommendations constitute the primary internationally recognised standards for the prevention and detection of money laundering and terrorist financing.

(b) The Company applies the following:

i. Exercises additional monitoring procedures and pays special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or apply inadequately the aforesaid recommendations.

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

iii. With the aim of implementing the above, the AMLCO consults 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 AMLCO assesses the risk from transactions and business relationships with persons from various countries and decides of the countries that inadequately apply the FATF's recommendations. According to the aforesaid decision of the AMLCO, the Company applies, when deemed necessary, enhanced due diligence measures for identifying and monitoring transactions of persons originating from countries with significant shortcomings in their legal and administrative systems for the prevention of money laundering and terrorist financing.