ISWM
Asset Management Ltd

(Authorised by the Cyprus Securities & Exchange Commission)

PREVENTION OF MONEY LAUNDERING & TERRORIST FINANCING (AML) MANUAL

MAY 2022

Table of Contents

1 General Definitions

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

"**Advisory Authority or MOKAS or Unit**" shall mean the Advisory Authority for Combating Money Laundering which is established under Section 56 of the AML Law.

"**Beneficial Owner or Ultimate Beneficial Owner or UBO**" shall mean any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted and includes at least:

a) In the case of corporate entities:

i. the natural person(s) 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 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 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 twenty five percent (25%) plus one (1) share or ownership interest of more than twenty-five percent (25%) in the customer held by a natural person; and
(b) an indication of indirect ownership shall be a shareholding of twenty five percent (25%) plus one (1) share or an ownership interest over twenty-five percent (25%) in the customer 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 furthermore that control by other means can be verified inter alia on the basis of the criteria set forth in Article 142 (1) (b) and 148 of the Companies Law.

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

Provided that control by other means may include, inter alia, the following:
- the control criteria that are used in the preparation of consolidated financial statements;
- through shares agreement;
- the exercise of dominant influence; or
- the power to appoint senior management members.

b) In the case of legal entities, such as foundations and legal arrangements, such as trusts, which administer and distribute funds:
(i) the settlor;
(ii) the trustee(s) or commissioner;
(iii) the protector, if any;
(iv) the beneficiaries, or where the individuals benefiting from the legal arrangement or 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.

c) In the case of legal entities such as foundations and legal arrangements similar to trusts, the natural person holding a corresponding or equivalent position with a person referred to in paragraph (b) shall be included;

"Board of Directors or BoD" shall mean the board, committee and/or body of an entity that has the power to set the strategy, objectives, and general direction of that entity and oversees and monitors management decision-making, including a person who effectively directs the business activities of that entity.

"**Business Relationship**" shall mean 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**" shall mean any legal or physical person aiming to conclude a Business Relationship or conduct an occasional transaction with the Company.

"Committee of Experts on the Evaluation of Anti-Money Laundering Measure (Moneyval)" means the permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the terrorist financing of terrorism and the effectiveness of their implementation.

"**Company or Firm or ISWM**" shall mean the ISWM Asset Management Ltd which is incorporated in the Republic of Cyprus with registration number HE411707.

"CySEC or Regulator" shall mean the Cyprus Securities and Exchange Commission.

"**Cryptoassets**" shall mean a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored, and traded electronically, and it is not –
(a) fiat currency, or
(b) electronic money, or
(c) financial instruments, as these are specified in Part III of the First Appendix to the Investment Services and the Activities and Regulated Markets Law

"**Directive or AML Directive**" shall mean the CySEC Directive for the Prevention of Money Laundering and Terrorist Financing of 2021, as in force and/or as this may be amended from time to time by CySEC.

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

"**EU Directive**" Directive 2018/843 of the European Parliament and of the Council of 30 May 2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2015/849 of the European Parliament and of the Council, and amending Directives 2009/138/EC and 2013/36/EU.

"FATF" refers to the Financial Action Task Force. An inter-governmental body responsible to develop policies to combat money laundering.

"**goAML Professional Edition (PE)**" means an IT system implemented by the Money Laundering Combat Unit of the Republic (hereinafter the "**Unit**") and used by the Company for the online submission of Suspicious Activities Reports and Suspicious Transactions Reports.

"high risk third country" means a third country, designated by the Commission pursuant to the provisions of section 9(2) of EU Directive by the issuance of acts by way of derogation, which presents strategical shortcomings in its national system for combating money laundering and terrorist financing which are considered as important threats for the financial system of the European Union, and a third country, which is categorised by the obliged entities as high risk in accordance with the risk assessment foreseen by section 58A, and as provided in Section 8.7.5. of this Manual;

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

"Independent and Reliable Sources", may be public or independent authorities (e.g. ministries issuing ID cards/passports or the Registrar of Companies in respect of legal persons). In the event where there is no Registrar of Companies or any other similar source of retaining companies' information in any jurisdiction, it may be acceptable to obtain evidence of identity documents or information from a regulated financial institution with the approval of MLCO.

"**Law or AML Law**" shall mean the Prevention and Suppression of Money Laundering Activities Law, Law 188(I)/2007-2021, as this is in force and/or as this may be amended/consolidated from time to time.

"**Legal Person**" shall mean any entity having legal personality, except for states or public bodies in the exercise of state authority and for public international organisations.

"**Manual**" shall mean the Company's AML Manual (this manual) in accordance with the CySEC Directive, as in force and/or as this may be amended from time to time by CySEC.

"**MOKAS**" shall mean the Unit for Combating Money Laundering which is established under Section 54 of the AML Law.

"Anti-Money Laundering Compliance Officer (AMLCO)" means the in-house person, which is responsible for discharging the AML Compliance Function.

"Money Laundering and Terrorist Financing (ML & TF)" means the money laundering offences and terrorist financing offences defined in Section 2 of the Law and described in Section 4 and 5 of the Law (laundering offences and predicate offences).

"**Money Laundering**" means the money laundering offences defined in Section 4 of the Law referred to also the following:
Every person a) knows or b) 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 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.

Further and for the purposes of the above:

i. It does not matter whether or not the predicate offence is subject to the jurisdiction of the Cyprus Courts;
ii. Laundering offenses may also be committed by perpetrators of predicate offences;
iii. The knowledge, intent or purpose required as elements of the offenses referred above, may be inferred/concluded from objective factual circumstances.
iv. no prior or simultaneous conviction is required for an offense giving rise to the offense income·
v. it is not necessary to prove the identity of the person who committed the offense revenue.

"**Obliged Entities**" are:

(a) Credit institutions;

(b) Financial institutions;

(c) Any of the following natural or legal persons in the exercise of their professional activities:

(i) Auditors, external accountants, tax advisors, and any other person who undertakes to provide, either directly or through other persons with whom this person is connected, material assistance, subscription or advice on tax issues, as his main business or professional activity;

(ii) independent legal professionals where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the:

a) buying and selling of real property or business entities

b) managing of client money, securities or other assets

c) opening or management of bank, savings or securities accounts

d) organisation of contributions necessary for the creation, operation, or management of companies

e) creation, operation, or management of trusts, companies, foundations, or similar structures

(d) (service providers) natural or legal persons not already covered under point (c) above which provide the following services to trusts or companies: company formation, provision of services or director or secretary, provision of services of registered office, provision of trustee services, provision of services of registered shareholder on behalf of third parties, any of the services or activities stated under section 4 of the Law Regulating Companies providing administrative services and related matters of 2012.

(e) Real Estate agents, including when these are acting as intermediaries for the rental of real estate only when the monthly rent is equal to or exceeds ten thousand euros (€ 10,000).

(f) Providers of gambling services.

(g) Casinos, which fall under the scope of The Casino Operation and Control Law of 2015.

(h) A person who trades goods, if the payment is made or received in cash and amounts to an amount equal to or greater than ten thousand euros (€ 10,000), regardless of whether the transaction is carried out in a single transaction or in several related transactions.

(i) Providers of services related to Crypto-Assets, which are registered in the register provided for in paragraph (1) of article 61E of the Law.

(j) Persons, whose supervision is assigned to the CySEC under the provisions of the Cyprus Securities and Exchange Commission Law or any other law.

(k) Persons who trade or act as intermediaries in the trade of works of art, including in the case of art galleries and auction houses, if the value of the transaction or series of related transactions amounts to or exceeds ten thousand euros (€ 10,000).

(l) Persons who store, trade or act as intermediaries in the trade of works of art carried out by free ports, if the value of the transaction or series of related transactions amounts to or exceeds ten thousand euros (€ 10,000).

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

"**Politically Exposed Persons (PEPs)**" means the natural persons who are or have been entrusted with prominent public functions in the Republic or in another country and their immediate family members or persons known to be close associates of such persons. Prominent public functions includes:

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

No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials;

- **"family members"** means 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;

- **"persons known to be close associates"** means: (a) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person; (b) natural persons who have 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" mean criminal offenses that constitute criminal offenses under the laws of the Republic of Cyprus. Further:

- A person who markets gems and / or precious metals, motor vehicles, works of art and / or antiques in the context of its business activities to collect cash amount equal to or greater than ten thousand euros (€ 10,000), irrespective of whether the transaction is carried out by a single act or by more than one act that appears to be related.

- A person who markets gems and / or precious metals, motor vehicles, works art and / or antiques, in breach of the prohibition set out in paragraph (1), commits a criminal offense and, if convicted, is subject to a fine not exceeding ten per cent (10%) of the amount received in cash.

"Proceeds" means any kind of property or economic benefit which has been generated directly or indirectly from the commission of illegal activities and includes every subsequent reinvestment or conversion of direct products and every substantial gain.

"Property" means assets of any kind, whether corporeal or incorporeal, movable assets including cash, immovable assets, tangible or intangible, crypto-assets, electronic money, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such asset.

"Report" refers to the annual report prepared by the AMLCO according to paragraph 10 of the Directive.

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

"Risk Assessment" means a process of evaluating the potential money laundering and terrorist financing risks that may be involved in a Client business relationship.

"**Senior Management**" means an officer or employee with sufficient knowledge of the Company's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, regardless of whether or not such person is a member of the Company's board of directors (provided that the 'senior management official' need not be a member of the board of directors of the obliged entity).

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

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

"Tipping off" means that no person should disclose any information to the Client or a third person which may cause obstruction or negatively interfere with interrogations and investigations carried out. This includes information relating to suspicious transactions that has been or will be transmitted to MOKAS.

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

2 Introduction

2.1 Purpose of the AML Manual

The aim of this Manual is to provide the guidelines that should be followed throughout the Company for the detection and/or prevention of money-laundering activities and terrorist financing.

The Manual lay down the Company's internal practices, measures, procedures and controls relevant to and in accordance with the Prevention and Suppression of Money Laundering Law (hereinafter referred to as the "**AML Law**"), as in force and/or as these may be amended/consolidated from time to time, and further to assist the Company's employees to achieve the following objectives:

- Maintain the integrity, credibility and reputation of the Firm;
- Implement and comply with all the legal and regulatory requirements that govern the operations of the Firm;
- Enable the tracking and identification of suspicious transactions/activities and protect the Firm from the possible fraud and risks involved in its financial strength and reputation;
- Be able to contribute to the investigation, if a client is investigated for money laundering, and submit data on the specific incident of money laundering;
- Provide and implement the processes for establishing business relationship, the execution of an Occasional Transaction and the monitoring processes for such relationship and transactions;
- Report any suspicious transactions for money laundering internally and externally to the appropriate authorities;
- Enable the development of the professional relationship with the client.

The Manual is developed and periodically updated by the Anti-Money Laundering Compliance Officer (hereinafter referred to as the "**AMLCO**") based on the general principles set up by the Company's Board of Directors (hereinafter referred to as the "**Board**" or "**BOD**") in relation to the AML Law. All amendments and/or changes of the Manual must be approved by the Board. The Manual shall be communicated by the AMLCO to all members of the BOD and the Company's employees that manage, monitor or control in any way the Clients' business relation and/or transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined herein. The Manual has been prepared to comply with the provisions of the AML Law, and the CySEC AML Directive.

The Manual applies to the services offered to the Company's Clients as well as the relevant Company's dealings with its Clients.

In this respect, the AMLCO shall be responsible to update the Manual so as to comply with CySEC's future requirements, as applicable, regarding the Client identification and due diligence procedures which a Company must follow. The AML Director has the responsibility of supervising that the AML Manual is updated on an ongoing basis.

2.2 Manual Applicability

All Company's employees should conduct themselves properly at all times and according to the highest standards of professionalism and integrity. No action may be taken that will reflect poorly on the Company. If there is any doubt about a particular course of action and its impact on the Company, employees should seek the advice of the AMLCO before proceeding. Each Company's employee has a fundamental duty to notify the AMLCO of any matters that may constitute a breach of these rules, policies and procedures, even if the employee only becomes aware of such a matter after the action has been taken.

The Board and in particular the AML Director nominated by the Board bear the responsibility for the adequacy of the processes and the control safeguards applied by this Manual and all internal policies and procedures of the Company. The Manual has been prepared so that it complies with, and applies, the principles of best practice in accordance to the relevant applicable laws and regulations of the Republic of Cyprus, as these may be amended from time to time.

Compliance with this Manual and all applicable laws, regulations and rules is an important condition of continued employment with the Company. Failure to comply either with the rules, policies and procedures set out in the Manual, or with the high standards of professionalism and integrity Company's employees are expected to exhibit, or with any relevant laws, regulations or rules may, in addition to putting an employee in breach of his or her contract of employment, result in sanctions from external regulators and in extreme cases prosecution. On joining the Company, each employee is required to sign an undertaking in the form set out in Appendix 5 of this Manual to acknowledge their understanding of this.

The Company maintains a register for the monitoring of future relevant legislative updates or amendments, as well as for the delivery of copies of the Manual and any further instructions and rules to all members of staff.

2.3 What is Money Laundering?

Money laundering is defined very widely, and includes any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources. It usually involves three stages:

a. **Placement** – Placement of illicit funds in the financial system
b. **Layering** – The actions of distancing illegally obtained proceeds from their source via the creation of multiple and complex levels of financial transactions designed to disguise the audit trail and to provide anonymity.
c. **Integration** – Re-entrance of the illicit funds in the financial system appearing to be legitimate proceeds.

In accordance with Section 5 of the Law, Predicate offences refers to any offence which is defined as a criminal offence by any law of the Republic.

Criminal property may take any form, including money, securities, tangible property and intangible property.

Illegal Activities can be generated for example through drug trafficking, illegal arms sales, smuggling, insider trading, embezzlement, bribery and internet fraud schemes and any offence punishable in the Republic by a term imprisonment exceeding one year.

As evident from the definition of the Predicate Offences, money laundering is also taken to encompass activities related to Terrorist Financing, including handling or possessing funds to be used for terrorist purposes as well proceeds from terrorism.

Businesses and individuals need to be alert of the risk of Clients, their counterparties and others laundering money in any of its possible forms as money laundering is not only about cash transactions. It can be achieved through virtually every medium and financial institution or business. The business or its Client does not have to be a party to money laundering for a reporting obligation to arise (see Section 12).

According to the definition of Money Laundering provided in Section 4(1) of the Law:
A person commits an offence when he/she:

- Knows or (*subjective factor*)
- Ought to have known (*objective factor*)

that any kind of property constitutes proceeds from the commission of a Illegal Activities and carries out any of the following activities listed below:

i. Converts, 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 (*aiding & abetting*)
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 (Tipping Off)

The above offences (i) to (v) are punishable by 14 years imprisonment and/or a penalty of up to €500,000 where a person 'knows' of a money laundering offence by 5 years imprisonment and/or a penalty of up to €50,000 where a person 'ought to have known'.

Further, Section 4(2) of the Law, stipulates that: for the purposes of Section 4(1) of the Law:

a) it shall not matter whether the illegal activities are subject to the jurisdiction of the Cyprus Courts or not.

b) a laundering offence may be committed by the offenders of a Predicate Offence as well;

c) the knowledge, intention or purpose which are required as elements of the offences referred to in Section 4(1) of the Law may be inferred from objective and factual circumstances;

d) There is no requirement for a prior or simultaneous conviction of a Predicate Offence, from which proceeds were derived;

e) There is no requirement to prove the identity of the person who committed the illegal activities from which proceeds were derived;

f) Conviction for the offences referred to in Section 4(1) of the Law is possible if, based on objective factual circumstances, it is proven that the property was derived from illegal activities, without the need to document all the actual evidence or all the circumstances related to these illegal activities.

A legal person may be liable for committing any of the offences referred to in Section 4(1) of the Law, committed for the benefit of any person acting individually or as a member of a body of the legal entity and holds a managerial position within it, on the basis of:

(i) power of representation of the legal person,

(ii) decision-making power on behalf of the legal person, or

(iii) power to exercise control within the legal person.

A legal person shall be liable for committing any of the offences referred to in Section 4(1) of the Law in the case that the absence of supervision or control by a person specified above made it possible for the offense to be committed in favour of that legal person by a person under its authority.

The liability of a legal person, as referred to above, does not preclude criminal prosecution of a natural person who is the perpetrator, abettor or accomplice in committing any of the offenses referred to in Section 4(1) of the Law.

In the event of a conviction for an offense provided for in points (i), (ii) or (iii) of Section 4(1) of the Law, the following circumstances are considered to be encumbering:

a) the crime was committed in the context of a criminal organisation – for the purposes of this section, "criminal organisation" has the meaning attributed to this term in Article 1 of the Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime";

b) the person is a liable entity and has committed the offense during the exercise of his professional activity;

c) the property that is the object of money laundering is of significant value.

In the event that the commission of any of the offenses provided for in Section 4(1) of the Law is subject to the jurisdiction of more than one Member States of the European Union and any of the Member States may validly prosecute on the basis of the same facts, Member States shall work together to decide which of them will proceed with the prosecution of the suspect, with a view to concentrate the proceedings in a single Member State – for the purposes of this, the following factors may be taken into account:

a) The Member State in whose jurisdiction the offense was committed;

b) the nationality or place of residence of the suspect;

c) the country of origin of the victim or victims; and

d) the Member State in whose jurisdiction the suspect was located.

It is further understood that, where appropriate and in accordance with Article 12 of the Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings", the issue is referred to in Eurojust – for the purposes of this section, "Eurojust" means the unit established by the Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime".

The Court may, in addition to the fine provided for above, impose to a legal person convicted of the offense of any of the above-mentioned offenses:

a) exclusion from public benefits or aid;

b) temporary or permanent exclusion from access to public funding, including tenders, grants and concessions;

c) temporary or permanent ban on commercial activity;

d) judicial liquidation; and

e) temporary or permanent closure of the premises used for committing the offense.

2.4 What is Terrorist Financing?

Terrorism is defined as the use or threat of action designed to influence government, or to intimidate any section of the public, or to advance a political, religious or ideological cause where the action would involve violence, threats to health and safety, damage to property or disruption of electronic systems.

The funding of terrorist organisations is made from both legal and illegal revenue generating activities. Funds obtained from illegal sources are laundered by terrorist groups by the same methods used by criminal groups. 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.

Funding for terrorist organizations is based on revenue derived from both legal and illegal sources. Criminal offenses include kidnapping (requiring ransom), extortion (demanding money for "protection"), smuggling, theft, burglary and drug trafficking.

Further information on the types of criminal offences that fall under terrorism and the corresponding sanctions can be found in the Combating of Terrorism and Victim Protection Law of 2019 (N.75(I)/2019).

Legal fund raising methods used by terrorist organizations include:

i. collecting subscriptions
ii. sale of books and other printed material
iii. cultural and social events
iv. donations
v. illegal fundraising from the community

Non-profit organizations

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

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

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

a) Use of funds by a non-profit organisation is not consistent with the purpose for which it was established.
b) Donations relating to a cause that is subject to derogatory publicly available information (crowdfunding initiative, charity, NPO, NGO, etc.).
c) A mismatch between the type and size of financial transactions and the stated purpose and activity of the non-profit organisation.
d) A sudden increase in the frequency and amounts of financial transactions for the account of a non-profit organisation.
e) Large and unexplained cash transactions by non-profit organisations.
f) The absence of contributions from donors located within the country of origin of the non-profit organisation.

The consequences of allowing the financial system to facilitate the movement of terrorist money are so horrendous that every effort must be made to prevent this from happening. So combating money laundering and financing of terrorism are not only the regulatory requirement but also an act of self-interest.

Therefore, the preventive measures covered by this Manual are intended not only to counter the use of the values derived from crime but also to prevent the implementation of any activities that could be tracked down to terrorism financing activities.

In order to tackle terrorism financing effectively, it is essential that the Company cooperates with MOKAS. It is also very important that investigation of terrorism cases at the national level include the terrorist-financing element.

In carrying out its tasks, the Company shall work closely with MOKAS in cases stipulated by law.

Difference between ML & TF Offences

In relation to money laundering, the proceeds have as a source, by definition, predicate (criminal) offences. In relation to terrorist financing offences, the money collected for terrorist financing, may come from completely legitimate sources.

Therefore, illegality in relation to money laundering is due to the sources of the money used, whereas illegality in relation to terrorist financing is due to the purpose the money collected is used.

3 THE RESPONSIBILITIES OF THE BOARD OF DIRECTORS

3.1 Board Responsibilities

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

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

(b) to appoint a senior official that possesses the skills, knowledge and expertise relevant to financial and other activities depending on the situation, who shall act as the AMLCO as well as an Alternate AMLCO who shall replace the AMLCO upon his absence and, where is necessary, assistant AMLCOs and determine their duties and responsibilities, which are recorded in this Manual,

(c) to appoint a Board member as the AML Director who shall remain ultimately responsible for the application of the provisions of the Law and of any instructions and / or circulars and / or regulations issued by virtue of the law, including any relevant acts of the European Union,

(d) to approve this Manual,

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

(f) to ensure that the AMLCO, the Alternate AMLCO and his assistants, if any, and any other person who has been assigned with the duty of implementing the procedures for the prevention of Money Laundering, have complete and timely access to all data and information concerning Clients' identity, transactions' documents (as applicable to the Company) and other relevant files and information maintained by the Company so as to be fully facilitated in the effective execution of their duties, as included herein,

(g) to ensure that all employees are aware of the person who has been assigned the duties of the AMLCO and Alternate AMLCO, as well as his assistants (if any), to whom they report, according to point (e) of Section 5.2 of the Manual any information concerning transactions and activities for which they have knowledge or suspicion that might be related to Money Laundering,

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

(i) to ensure that the AMLCO has sufficient resources, including competent staff and technological equipment, and receive all necessary training and support for the effective discharge of their duties,

(j) to assess and approve the AMLCO's Annual Report of Section 5.4 of the Manual and take all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the abovementioned report. The minutes of the said decision of the Board and the AMLCO's report shall be submitted to CySEC no later than three (3) months after the end of the calendar year (i.e. the latest, by the end of March),

(k) to meet and decide the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected in the Internal Auditor's report in the manner described in Section 4 of the Manual. The minutes of the said decision of the Board and the Internal Auditor's report shall be submitted to CySEC within 20 days of the said meeting and no later than four (4) months after the end of the calendar year (i.e. the latest, by the end of April),

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

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

(n) to ensure that the Company during the performance of the procedures for prescribed in this Manual complies will all obligations emanating from EU General Data Protection Regulation ("**GDPR Regulation**"),

(o) approve the mandatory annual training programme prepared by the AMLCO,

(p) ensure that it receives adequate management information on the implementation of the regulated entity's AML/CFT training programme, and

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

3.2 AML Director

A member of the Board shall be responsible for the implementation of the provisions of the Prevention and Suppression of Money Laundering and Terrorist Financing Laws of 2007 – 2018 and of the directives and/or circulars and/or regulations issued pursuant thereto including any relevant acts of the European Union.

More specifically, the AML Director shall bear the responsibility of, *inter alia*, the following duties on ongoing basis:

(a) supervising that all requirements of the Law and the relevant CySEC directives and circulars are applied,
(b) supervising the activities of the personnel of the Anti – Money Laundering Department,
(c) supervising the ongoing implementation of the provisions of the AML manual and relevant reporting to Compliance Officer, Risk Manager and/or BOD,
(d) supervising that the AML Manual is updated on an ongoing basis so as to comply with the CySEC's future requirements, as applicable, regarding the Client identification and due diligence procedures,
(e) understanding and developing knowledge of regulatory guidelines and how they influence Company's business processes with the assistance of the Compliance Officer,
(f) supervising the duties of the MLCO and, assistant AMLCOs and responsibilities, which are recorded in the risk management and procedures manual regarding money laundering and terrorist financing,
(g) supervising the preparation of the Annual report of the AMLCO,
(h) ensuring that the appropriate means and training is provided to Company's employees in relation to Anti – Money Laundering in order for them to carry out their duties successfully and in compliance with relevant laws and regulations,
(i) supervising the reports of suspicious transactions to Unit for Combating Money Laundering (MOKAS),
(j) supervising the preparation of the Monthly Prevention Statement and its submission to CySEC via CySEC's Portal,
(k) ensuring that the AMLCO and his assistance, if any, and any other person who has been assigned with the duty of implementing the procedures for the prevention of money laundering and terrorist financing, shall have complete and timely access to all data and information concerning Clients' identity, transaction documents and other relevant files and information maintained by the Company so as to be fully facilitated in the effective execution of their duties,
(l) supervising the implementation of the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected in the Internal Auditor's report,
(m) supervising the implementation of the Client Acceptance Policy (CAP),
(n) receiving on periodic basis information from the employees of the Company in relation to the ongoing monitoring of high risk Clients' transactions and activities and ensure that the relevant guidance is provided by the AMLCO, as and where needed,
(o) supervising and assessing the correct and effective implementation of the internal practices mentioned in AML/CFT Manual, for the proper and full implementation of the Company's obligations and/or procedures, where the verification of a Client's identity takes place during the establishment of business relationship,

(p) supervising that the AMLCO applies all the appropriate monitoring mechanisms (e.g. on-site visits to different departments of the Company) which will provide him with all the necessary information for assessing the level of compliance of the departments and employees of the Company with the procedures and controls, which are in force, and

(q) supervising that in the event that the AMLCO identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, he/she gives appropriate guidance for corrective measures and informs the Board accordingly.

4 OBLIGATIONS OF THE INTERNAL AUDITOR

4.1 General

The following obligations of the Internal Auditor are addressed specifically for the prevention of Money Laundering and Terrorist Financing:

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

b) the findings and observations of the internal auditor, in relation to point (a) above, shall be submitted, in a written report form, to the Board.

5 ANTI-MONEY LAUNDERING COMPLIANCE OFFICER (AMLCO)

5.1 General

The AMLCO must be a senior management official with sufficient skills, experience and knowledge in AML/CTF and Compliance areas, as well as knowledge of the Company, its service lines and its clients. Furthermore, the AMLCO shall lead the Company's Money Laundering Compliance procedures and processes and report to the Senior Management. The AMLCO shall also have access to all relevant information necessary to perform his duties adequately and effectively.

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

The AMLCO is replaced upon his absence by the Alternate AMLCO who undertakes to perform all AMLCO duties and responsibilities during the absence of the AMLCO. All references to AMLCO in this Manual refer also to the Alternate AMLCO when replacing the AMLCO. The Alternate AMLCO is appointed by the Board and shall be an employee of the Company or an external consultant with adequate knowledge, skills and experience in order to discharge the respective duties.

5.2 Duties of the AMLCO

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

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

(a) to design, based on the general policy principles of the Company mentioned in point (a) of Section 3.1 of the Manual, the internal practice, measures, procedures and controls relevant to the prevention of money laundering and terrorist financing, and describe and explicitly allocate the appropriateness and the limits of responsibility of each department that is involved in the abovementioned

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

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

(d) to monitor and assess the correct and effective implementation of the policy mentioned in point (a) of Section 3.1 of the Manual, the practices, measures, procedures and controls of point (a) above and in general the implementation of the Manual. In this respect, the AMLCO shall apply

appropriate monitoring mechanisms (e.g. on-site visits to different departments of the Company) which will provide him with all the necessary information for assessing the level of compliance of the departments and employees of the Company with the procedures and controls which are in force. In the event that the AMLCO identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, gives appropriate guidance for corrective measures and where deems necessary informs the Board

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

(f) to evaluate and examine the information received as per point (e) above, by reference to other relevant information and discuss the circumstances of the case with the informer and where appropriate, with the informer's superiors. The evaluation of the information of point (e) above shall be done on a report (hereinafter the "**Internal Evaluation Report**"), a specimen of such report is attached in Appendix 2 of the Manual

(g) if following the evaluation described in point (f) above, the AMLCO decides to notify the Money Laundering Combat Unit of the Republic (hereinafter the "Unit"), then he should complete a written report and submit it to the Unit the soonest possible via the goAML (https://reports.mokas.law.gov.cy/live) to which the Company has registered.

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

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

(j) to ensure the preparation and maintenance of the lists of Clients categorised following a risk based approach, which contains, among others, the names of Clients, their account number and the dates of the commencement of the Business Relationship. Moreover, the AMLCO ensures the updating of the said list with all new or existing Clients, in the light of any additional information obtained. This is then reviewed and monitored by the AMLCO on an ongoing basis

(k) to assess and categorize all new Clients depending on their level of Risk according to the provisions of Sections 7.3 of this Manual

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

(m) to evaluate the systems and procedures applied by a third person on whom the Company may rely for Client identification and due diligence purposes, according to Section 8.9 of the Manual, and approves the cooperation with it (if and where applicable)

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

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

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

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

(r) to prepare correctly and submit timely to CySEC the monthly prevention statement of Section 5.5 of the Manual and provide the necessary explanation to the appropriate employees of the Company for its completion

(s) to prepare the Annual Report, according to Section 5.4 of the Manual
(t) to respond to all requests and queries from the Unit and CySEC, provide all requested information and fully cooperate with the Unit and CySEC
(u) to maintain a registry which includes the reports of points (f), (g) and (h), and relevant statistical information (e.g. the department that submitted the internal report, date of submission to the AMLCO, date of assessment, date of reporting to the Unit), the evaluation reports of point (i) and all the documents that verify the accomplishment of his duties
(v) (if ever applicable to the Company) maintain a record of the data / information of third parties, which the Company relies upon the for the identification and due diligence measures customer pursuant to Section 67 of the Law, as specified in paragraph 25 of the Directive.

Further, the AMLCO shall monitor and evaluate, on an on-going basis, the effectiveness of the measures and procedures of Section 6 of the Manual.

5.3 Duties of the Alternate AMLCO

The Alternate AMLCO should replace AMLCO during his absence and should remain responsible for the discharge of all duties and responsibilities of the AMLCO. The Alternate AMLCO should therefore meet the conditions for the appointment of an AMLCO as provided by CySEC's directives and circulars. It is clarified that Alternate AMLCO replaces the AMLCO only during his absence. When the AMLCO resigns the Company should proceed with appointing a new AMLCO.

5.4 Annual Report of the AMLCO

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

The AMLCO's Annual Report shall be prepared and be submitted to the Board for approval within two (2) months from the end of each calendar year (i.e. at latest, by the end of February each year).

Following the Board's approval of the Annual Report, a copy of the Annual Report should be submitted to CySEC together with the Board's meeting minutes no later than three (3) months from the end of each calendar year (i.e. at latest, by the end of March).

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

(a) information for measures taken and/or procedures introduced for compliance with any amendments and/or new provisions of the Law and the Directive which took place during the year under review
(b) sufficiently analytical reference/information on the inspections and reviews performed by the AMLCO to determine the degree of compliance of the Company and its policies, practices, measures, procedures and controls applied for the prevention of money laundering reporting the material deficiencies and weaknesses identified in the policy, practices, measures, procedures and controls that the Company applies for the prevention of Money Laundering and Terrorist Financing. In this respect, the report outlines to a sufficient extent the seriousness of the deficiencies and weaknesses, the risk implications and the actions taken and/or recommendations made for rectifying the situation
(c) the number of Internal Suspicion Reports submitted by Company personnel to the AMLCO, according to point (f) of Section 5.2 of the Manual and possible comments/observations thereon
(d) the number of reports submitted by the AMLCO to the Unit, according to point (g) of Section 5.2 of the Manual with information/details on the main reasons for suspicion and highlights of any particular trends
(e) information, details or observations regarding the communication with the employees on money laundering preventive issues
(f) summary figures, on an annualised basis, of Clients' total cash deposit in Euro and other currencies in excess of the set limit of €10,000 (together with comparative figures for the previous

year) as reported in the monthly prevention statement of Section 5.5 of the Manual. Any comments on material changes observed compared with the previous year are also reported

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

(h) Sufficient reference to information on the systems and procedures applied by the Company for the ongoing monitoring of Client accounts and transactions and transactions that are compared with the data kept in their economic profile, including in addition, sufficient reference to the method of documenting the ongoing monitoring of customers' accounts and transactions and to the results of the ongoing monitoring of customers' accounts and transactions during the year.

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

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

(k) information on training/education and any educational material provided to staff during the year, reporting, the number of courses/seminars organised, their duration, the number and the position of the employees attending, the names and qualifications of the instructors, and specifying whether the courses/seminars were developed in-house or by an external organization or consultants, including also sufficient reference to the specific method with which the adequacy and effectiveness of staff training has been assessed and reference to the results. (l) results of the assessment of the adequacy and effectiveness of staff training

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

(m) 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

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

(o) relevant BoD minutes accompanying the AMLCOs' Annual Reports, should include implementation timeframes of the measures decided for the correction of the weaknesses and/or deficiencies identified in these reports

5.5 Monthly Prevention Statement (MPS)

The AMLCO shall prepare and submit to CySEC, according to point (r) of Section 5.2. above, on a monthly basis, the CySEC Form 144-08-11 "Monthly prevention statement regarding the prevention of Money Laundering and Terrorist Financing", which includes details for the total cash deposits accepted by the Company. The aforementioned Form must be completed and submitted to CySEC within fifteen (15) days from the end of each month.

The scanned copy of the duly completed and signed Form 144-08-11 should be submitted to CySEC only electronically via CySEC's Portal. The original completed and signed form must be kept in the Company's offices.

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

The Internal Auditor shall be responsible to review, at least annually as per Section 4 of the Manual, the submission to CySEC of the "Monthly prevention statement regarding the prevention of Money Laundering and Terrorist Financing".

6 Risk – Based Approach (RBA)

6.1 Risk – Based Approach – General Framework

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

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

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

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

The risk-based approach adopted by the Company, and described in the Manual, involves specific measures and procedures in assessing the most cost effective and appropriate way to identify and manage the Money Laundering and Terrorist Financing risks faced by the Company.

Such measures include:

(a) identifying and assessing the Money Laundering and Terrorist Financing risks emanating from particular Clients or types of Clients, services, and geographical areas of operation of its Clients
(b) Adherence to the policies, procedures and controls in place by the Risk Management, Compliance and Anti-Money Laundering Officer managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls
(c) continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

The application of appropriate measures and the nature and extent of the procedures on a risk-based approach depends on different indicators. Such indicators include the following:

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

When assessing the risk of money laundering and terrorist financing the Company takes into account, among others, the Risk Factor Guidelines and any guidelines/guidance issued by the Financial Action Task Force (FATF).

The AMLCO shall be responsible for the development of the policies, procedures and controls on a risk-based approach. Further, the AMLCO shall also be responsible for the implementation of the policies, procedures and controls on a risk-based approach. The Internal Auditor shall be responsible for reviewing the adequate implementation of a risk-based approach by the AMLCO, at least annually, as per Section 4.1 of the Manual.

6.2 Risk – Based Approach (RBA) - Identification of Company's Risks

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

The Company performs a business-wide risk assessment to understand where it is exposed to money laundering risks and which areas of its business should prioritise in the fight against the said risks, as well as individual risk assessments to understand where it is exposed to money laundering and terrorist financing risks as a result of entering into a business relationship or carrying out an occasional transaction. The Company identifies the risk factors and assess the money laundering and terrorist financing risk associated with the products and services it offers, the jurisdictions it operates in, the customers it attracts and the delivery channels used to service its clients.

When assessing the overall level of residual ML/TF risk associated with its business and with individual business relationships or occasional transactions, the Company shall consider both, the level of inherent risk, and the quality of controls and other risk mitigating factors.

When identifying the risk associated with its products, services or transactions, the Company considers the risks related to:

(a) the level of transparency, or opaqueness, the product, service/transaction affords;
- To what extent do products or services allow the client 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?

(b) the complexity of the product, service/transaction;
- How complex is the transaction and does it involve multiple parties or multiple jurisdictions, for example in the case of certain trade finance transactions? Are transactions straightforward, for example are regular payments made into a pension fund?
- 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 Company 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 client's own account at another financial institution that is subject to AML/CFT standards and oversight that are comparable to those required under Directive?
- Does the firm 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?

(c) the value or size of the product, service/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?

(d) the way in which the client obtains the products or services they require, firms should consider the risk related to:

- Is the client 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 client 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 client 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 IV AML Directive?
- Has the client been introduced by a third party, for example a bank that is not part of the same group or an intermediary, and if so:
    - is the third party a a regulated person subject to AML obligations that are consistent with those of Directive (EU) 2015/849, and is the third party afinancial institution or is its main business activity unrelated to financial service provision?
    - does the third party apply CDD measures, keep records to EEA standards, is supervised for compliance with comparable AML/CFT obligations in line with Article 26 of Directive (EU) 2015/849, and are there any indications that the third party's level of compliance with applicable AML/CFT legislation or regulation is inadequate, for example whether the third party has 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 CEU Commission has identified as having strategic deficiencies, the Company must not rely on that third party. 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 Compnay is confident that the intermediary fully complies with group-wide policies and procedures in line with Article 45 of Directive (EU) 2015/849.
    - what has the Company done to be satisfied that:
        - the third party always provides the necessary identity documentation?
        - the third party will provide, immediately upon request, relevant copies of identification and verification data or electronic data referred to, inter alia, in Article 27 of Directive (EU) 2015/849?
        - the quality of the third party's CDD measures is such that it can be relied upon?
        - the level of CDD applied by the third party is commensurate to the ML/TF risk associated with the business relationship, considering that the third party will have applied CDD measures for its own purposes and, potentially, in a different context?
- Has the client been introduced through a tied agent, that is, without direct firm contact? To what extent can the Company be satisfied that the agent has obtained enough information so that the Company knows its client 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 Company's knowledge of the client and ongoing risk management?
- Where a firm uses an an outsourced service provider for aspects of its AML/CFT obligations, to the extent permitted by national legislation, has the Company considered whether the outsourced service provider is an obliged entity, and whether it has addressed the risks set out in the EBA's Guidelines on outsourcing (EBA/GL/2019/02), where those Guidelines are applicable? .

When identifying the risk associated with its Clients, including their clients' beneficial owners, the Company considers the risks associated:

a. with the client's and the client's beneficial owner's business or professional activity, such as:
    - Does the client or beneficial owner have links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the extractive industries or public procurement?

- Does the client 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 client or beneficial owner have links to sectors that involve significant amounts of cash?
- Where the client 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 client have political connections, for example, are they a Politically Exposed Person (PEP), or is their beneficial owner a PEP? Does the client or beneficial owner have any other relevant links to a PEP, for example are any of the client's directors PEPs and, if so, do these PEPs exercise significant control over the client or beneficial owner? Where a client or their beneficial owner is a PEP, firms must always apply EDD measures in line with Article 20 of AML IV Directive?
- Does the client 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 client a legal person subject to enforceable disclosure requirements that ensure that reliable information about the client's beneficial owner is publicly available, for example public companies listed on stock exchanges that make such disclosure a condition for listing?
- Is the client 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 client 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 client a public administration or enterprise from a jurisdiction with low levels of corruption?
- Is the client'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 client's or beneficial owner's source of wealth?

b. the client's and the client's beneficial owner's reputation, such as:

    - Are there adverse media reports or other relevant sources of information about the client, for example are there any allegations of criminality or terrorism against the client or the beneficial owner? If so, are these reliable and credible? Firms 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. Firms should note that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing.
    - Has the client, 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 client 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 client 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 client's or the beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship?

c. the client's and the client's beneficial owner's nature and behavior:
    - Does the client 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 client's or beneficial owner's identity?
- Are there indications that the client might seek to avoid the establishment of a business relationship? For example, does the client 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 client's ownership and control structure transparent and does it make sense? If the client's ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?
- Does the client issue bearer shares or does it have nominee shareholders?
- Is the client a legal person or arrangement that could be used as an asset-holding vehicle?
- Is there a sound reason for changes in the client's ownership and control structure?
- Does the client 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 client is trying to evade specific thresholds such as those set out in Article 11(b) of IV AML Directive and national law where applicable?
- Does the client request unnecessary or unreasonable levels of secrecy? For example, is the client reluctant to share CDD information, or do they appear to want to disguise the true nature of their business?
- Can the client'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 client use the products and services they have taken out as expected when the business relationship was first established?
- Where the client is a non-resident, could their needs be better serviced elsewhere? Is there a sound economic and lawful rationale for the client requesting the type of financial service sought?
- Is the client or the beneficial owner a person included in the lists of persons, groups and entities involved in terrorist acts and subject to restrictive measures, or are they known to have close personal or professional links to persons registered on such lists (for example, because they are in a relationship or otherwise live with such a person)?
- Is the client or the beneficial owner a person who is publicly known to be under investigation for terrorist activity or has been convicted for terrorist activity, or are they known to have close personal or professional links to such a person (for example, because they are in a relationship or otherwise live with such a person)?
- Does the client carry out transactions that are characterised by incoming and outgoing fund transfers from and/or to countries where groups committing terrorist offences are known to be operating, that are known to be sources of terrorist financing or that are subject to international sanctions? If so, can these transfers be explained easily through, for example, family ties or commercial relationships?
- Is the client a non-profit organization:
    - whose activities or leadership been publicly known to be associated with extremism or terrorist sympathies?
    - whose transaction behaviour is characterised by bulk transfers of large amounts of funds to jurisdictions associated with higher ML/TF risk and high-risk third countries?
- Does the client carry out transactions characterised by large flows of money in a short period of time, involving non-profit organisations with unclear links (e.g. they are domiciled at the same physical location; they share the same representatives or employees or they hold multiple accounts under the same names)?

- Does the client transfer or intend to transfer funds to persons included in the lists of persons, groups and entities involved in terrorist acts and subject to restrictive measures, or are they known to have close personal or professional links to persons registered on such lists, and who are publicly known to be under investigation for terrorist activity or have been convicted for terrorist activity, or they are known to have close personal or professional links to such a person?

Risk associated with countries and geographical areas:

a. the jurisdictions in which the client is based or is resident, and beneficial owner is resident;

b. the jurisdictions that are the client's and beneficial owner's main places of business; and

c. the jurisdictions to which the client and beneficial owner have relevant personal or business links, or financial or legal interests.

For Example:

- Has the country been identified by the Commission as having strategic deficiencies in its AML/CTF regime, in line with Article 9 of IV AML Directive? In these cases, the Company shall apply EDD measures in relation to high-risk third countries.
- Does the country's law prohibit the implementation of group-wide policies and procedures and in particular are there any situations in which the Commission Delegated Regulation (EU) 2019/758 should be applied?
- 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), the FATF's list of high-risk and non- cooperative jurisdictions, International Monetary Fund (IMF) assessments and Financial Sector Assessment Programme (FSAP) reports. The Company should note 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.
- 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 either from official sources, or from organised groups or organisations within that jurisdiction?
- Is there information, for example from law enforcement or credible and reliable open media sources, suggesting 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?
- 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; assessments conducted with regard to the EU list of non-cooperative jurisdictions for tax purposes; 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?
- Is there information from credible and reliable public sources about the level of predicate offences to money laundering listed in Article 3(4) of AML IV 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?

The nature and purpose of the business relationship shall determine the relative importance of individual country and geographical risk factors mentioned above. For example:

- 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 client 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 client is a trust of any other type of legal arrangement, or has a structure of functions similar to trusts such as, fiducie, fideicomiso, Treuhand, the Company should take into account the extent to which the country in which the client, and where applicable, the beneficial owner are registered effectively complies with international tax transparency and information sharing standards.

The Company assess and evaluates the risks it faces, for the use of its services for the purpose of Money Laundering. The particular circumstances of the Company determine suitable procedures and measures that need to be applied to counter and manage risk.

The financial instruments in relation to which the services are provided are mostly non-complex, involving relatively few Clients or Clients with similar characteristics, then the Company shall apply such procedures which are able to focus on those Clients who fall outside the 'norm'.

Company's Risks

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

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

- Customers with income and/or wealth from high-risk sectors such as the extractive industries, construction;
- Customers about whom credible allegations of wrongdoing have been made;
- Customers who expect unusually high levels of confidentiality or discretion;
- Customers whose spending or transactional behaviour makes it difficult to establish 'normal', or expected patterns of behavior;
- Very wealthy and influential clients, including customers with a high public profile, non-resident customers and PEPs;
- The customer requests that the firm facilitates the customer being provided with a product or service by a third party without a clear business or economic rationale;
- Non face-to-face Clients;
- Client transactions where there is no apparent legal financial/commercial rationale;

- Situations where the origin of wealth and/or source of funds cannot be easily verified;
- Unwillingness of Clients to provide information on the Beneficial Owners of a legal person;
- Clients introduced by a third person.

(b) *Risks based on the Company's products and services (if and as applicable):*

- customers requesting large amounts of cash or other physical stores of value such as precious metals;
- very high-value transactions;
- financial arrangements involving jurisdictions associated with higher ML/TF risk (firms should pay particular attention to countries that have a culture of banking secrecy or that do not comply with international tax transparency standards);
- lending (including mortgages) secured against the value of assets in other jurisdictions, particularly countries where it is difficult to ascertain whether the customer has legitimate title to the collateral, or where the identities of parties guaranteeing the loan are hard to verify;
- the use of complex business structures such as trusts and private investment vehicles, particularly where the identity of the ultimate beneficial owner may be unclear;
- business taking place across multiple countries, particularly where it involves multiple providers of financial services;
- cross-border arrangements where assets are deposited or managed in another financial institution, either of the same financial group or outside of the group, particularly where the other financial institution is based in a jurisdiction associated with higher ML/TF risk. Firms should pay particular attention to jurisdictions with higher levels of predicate offences, a weak AML/CFT regime or weak tax transparency standards.

6.3 RBA – Design and Implementation of Measures and Procedures to Manage and Mitigate the Risks

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

These measures and procedures include:

- adaption of the Client Due Diligence Procedures in respect of Clients in line with their assessed Money Laundering 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 (i.e. a holistic view of Client's activities) 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' relationship and transactions, as applicable to the Company.

In this respect, it is the duty of the AMLCO to develop and constantly monitor and adjust the Company's policies and procedures with respect to the Client Acceptance Policy and Client Due Diligence and Identification Procedures of Section 8 of the Manual, as well as via a random sampling exercise as regards existing Clients. These actions shall be duly documented and form part of the Annual Money Laundering Report, as applicable.

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

The AMLCO prepares and maintains a list of clients, which contain, inter alia, the clients' names, account numbers, and date of commencement of business relationship. The said list should be promptly updated

with all new or existing clients that the Company has determined, in the light of additional information received, that fall under one of the risk categories.

The Company monitors and evaluates, on an ongoing basis, the effectiveness of the measures and procedures that have been introduced for compliance purposes.

6.4 Risk Assessments

6.4.1 *Business-wide risk assessments*

Business-wide risk assessments shall help the Company understand where they are exposed to ML/TF risk and which areas of their business they shall prioritise in the fight against ML/TF. To this end, the Company shall take a holistic view of the ML/TF risks to which they are exposed, by identifying and assessing the ML/TF risk associated with the products and services they offer, the jurisdictions they operate in, the customers they attract and the transaction or delivery channels they use to service their customers.

The Company shall:

(a) identify risk factors based on information from a variety of internal and external sources, including the sources listed in Guidelines 1.30 to 1.31 from the Risk Factor Guidelines;
(b) have regard to relevant risk factors in Titles I and II of the Risk Factor Guidelines;
(c) take into account wider, contextual, factors such as sectoral risk and geographical risk, that could have a bearing on its ML/TF risk profile.

The Company shall ensure that its business-wide risk assessment is tailored to its business profile and takes into account the factors and risks specific to the Company's business, whether the Company draws up its own business-wide risk assessment or contracts an external party to draw up its business-wide risk assessment. Similarly, where the Company is part of a group that draws up a group-wide risk assessment, the Company shall consider whether the group-wide risk assessment is sufficiently granular and specific to reflect the Company's business and the risks to which it is exposed as a result of the group's links to countries and geographical areas, and complement the group-wide risk assessment if necessary. If the group is headquartered in a country associated with a high level of corruption, the Company shall reflect this in its risk assessment even if the group-wide risk assessment stays silent on this point.

A generic ML/TF risk assessment that has not been adapted to the specific needs and business model of the Company ('an off-the-shelf ML/TF risk assessment'), or a group-wide risk assessment that is applied unquestioningly, is unlikely to meet the requirements in Article 8 of Directive (EU) 2015/849.

As set out in Article 8 of Directive (EU) 2015/849, the steps the Company takes to identify and assess ML/TF risk across its business must be proportionate to its nature and size. Small firms that do not offer complex products or services and that have limited or purely domestic exposure, may not need a complex or sophisticated risk assessment.

The Company shall:

(a) make their business-wide risk assessment available to competent authorities;
(b) take steps to ensure that staff understand the business-wide risk assessment, and how it affects their daily work in line with Article 46 (1) of Directive (EU) 2015/849; and
(c) inform senior management about the results of their business-wide risk assessment, and ensure that senior management is provided with sufficient information to understand, and take a view on, the risk to which their business is exposed.

The Company shall record and document its business-wide risk assessment, as well as any changes made to this risk assessment in a way that makes it possible for the Company, and for competent authorities, to understand how it was conducted, and why it was conducted in a particular way.

6.4.2 *Individual risk assessments*

The Company shall find out which ML/TF risks it is, or would be, exposed to as a result of entering into, or maintaining, a business relationship or carrying out an occasional transaction. When identifying ML/TF risks associated with a business relationship or occasional transaction, the Company shall consider relevant risk factors including who their customer is, the countries or geographical areas it operates in, the particular products, services and transactions the customer requires and the channels the Company uses to deliver these products, services and transactions.

6.4.3 *Linking the business-wide and individual risk assessments*

The Company shall use the findings from its business-wide risk assessment to inform its AML/CFT policies, controls and procedures, as set out in Article 8(3) and (4) of Directive (EU) 2015/849. The Company shall ensure that its business-wide risk assessment also reflects the steps taken to assess the ML/TF risk associated with individual business relationships or occasional transactions and its ML/TF risk appetite.

To comply with the above, and also having regard to Section 6.4.2., the Company shall use the business-wide risk assessment to inform the level of initial customer due diligence that it will apply in specific situations, and to particular types of customers, products, services and delivery channels. Individual risk assessments should inform, but are no substitute for, a business-wide risk assessment.

6.4.4 *Keeping risk assessments up to date*

The Company shall put in place systems and controls to keep its assessments of the ML/TF risk associated with its business, and with its individual business relationships under review to ensure that its assessment of ML/TF risk remains up to date and relevant.

The systems and controls that the Company shall put in place to ensure its individual and business-wide risk assessments remain up to date shall include:

(a) Setting a date for each calendar year on which the next business-wide risk assessment update will take place, and setting a date on a risk sensitive basis for the individual risk assessment to ensure new or emerging risks are included.
(b) Where the Company becomes aware before that date that a new ML/TF risk has emerged, or an existing one has increased, this shall be reflected in its individual and business-wide risk assessments as soon as possible.
(c) Carefully recording issues throughout the relevant period that could have a bearing on risk assessments, such as internal suspicious transaction reports, compliance failures and intelligence from front office staff.

As part of this, the Company shall ensure that it has systems and controls in place to identify emerging ML/TF risks and that it can assess these risks and, where appropriate, incorporate them into its business-wide and individual risk assessments in a timely manner.

The systems and controls that the Company shall put in place to identify emerging risks should include:

(a) Processes to ensure that internal information, such as information obtained as part of the Company's ongoing monitoring of business relationships, is reviewed regularly to identify trends and emerging issues in relation to both, individual business relationships and the Company's business.
(b) Processes to ensure that the Company regularly reviews relevant information sources and in particular:
    i. in respect of individual risk assessments:
        - terror alerts and financial sanctions regimes, or changes thereto, as soon as they are issued or communicated and ensure that these are acted upon as necessary; and

- media reports that are relevant to the sectors or jurisdictions in which the Company is active.

ii. in respect of business-wide risk assessments:

- law enforcement alerts and reports;
- thematic reviews and similar publications issued by competent authorities; and
- processes to capture and review information on risks, in particular risks relating to new categories of customers, countries or geographical areas, new products, new services, new distribution channels and new compliance systems and controls.

(c) Engagement with other industry representatives and competent authorities (e.g. round tables, conferences and training), and processes to feed back any findings to relevant staff.

The Company shall determine the frequency of wholesale reviews of its business-wide and individual risk assessments methodology on a risk-sensitive basis.

6.5 Relevant International Organisations

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

(d) FATF - www.fatf-gafi.org
(e) The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (hereinafter "MONEYVAL") - www.coe.int/moneyval
(f) The EU Common Foreign & Security Policy (CFSP)- http://ec.europa.eu/cfsp/
(g) The UN Security Council Sanctions Committees - www.un.org/sc/committees
(h) The International Money Laundering Information Network (IMOLIN) - www.imolin.org
(i) The International Monetary Fund (IMF) – www.imf.org.
(j) The Joint Committee of the European Supervisory Authorities - https://esas-joint-committee.europa.eu/
(k) the EU Sanctions Map - https://www.sanctionsmap.eu/#/main
(l) the Ministry of Exterior in relation to International Sanctions by a relevant Decision/Resolution adopted by the Security Council (SC/UN), under chapter VII of the UN Charter; and Restrictive Measures adopted by the Council of the EU http://www.mfa.gov.cy/mfa/mfa2016.nsf/mfa35_en/mfa35_en?OpenDocument

7 CLIENT ACCEPTANCE POLICY

7.1 General

The Client Acceptance Policy (hereinafter the "**CAP**"), following the principles and guidelines described in this Manual, defines the criteria for accepting new Clients and defines the Client categorization criteria which shall be followed by the Company and especially by the employees which shall be involved in the Client Account Opening process. The following sections shall apply both to the onboarding of investors and funds under management. In the case of the latter, the Company shall, for every new fund it onboards, enter into the relevant fund management agreement on terms to be negotiated with each particular fund and request from the fund to fill-in the sign the relevant AIF/RAIF on-boarding questionnaire.

The AMLCO shall be responsible for applying all the provisions of the CAP.

The Internal Auditor shall review and evaluate the adequate implementation of the CAP and its relevant provisions, at least annually, as per Section 4 of the Manual.

7.2 Basic Principles of the CAP

The General Principles of the CAP are the following:

(a) the Company shall classify Clients into various risk categories and based on the risk perception decide on the acceptance criteria for each category of Client

(b) where the Client is a prospective Client, the Client must be accepted only after the relevant client onboarding due diligence and identification measures and procedures have been conducted, according to the principles and procedures set in Section 8 of the Manual

(c) all documents and data described in Section 8 of the Manual must be collected before accepting a new Client

(d) no account shall be opened or maintained in anonymous or fictitious names(s) or numbered accounts or accounts in names other than those stated in official identity documents or anonymous safes

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

- the AMLCO
- the Managing Director

Inadequate understanding of the client's profile and purpose of investment activity may expose the Company to a number of risks.

The CAP incorporates the following:

- The criteria for accepting new clients;
- Categories of clients who are not acceptable for establishing a business relationship or an execution of an occasional transaction;
- Criteria for categorization of clients on a risk basis in three categories (i.e. low risk, normal risk or high risk).

The principle of "Know Your Client" (KYC) should be applied. KYC processes are intended to enable a company to form a reasonable belief that it knows the true identity of each Client before the Client enters into a Business Relationship with the Company. The need to really KYC is at the very foundation of a good anti-money laundering management system. KYC due diligence is a continuous process and not only limited to Clients seeking to open new accounts. While Client identification procedures are aimed at establishing Clients' identity, the Company is also required to decide if the clients' risk-profile necessitate enhanced due diligence procedures.

The Company should not establish a relationship with a Client until it knows the Client's true identity.

The verification of identity of a Client/Beneficial Owner, takes place before the establishment of a Business Relationship with the said person.

By way of derogation to the general rule of article 62(1) of the Law, the verification of identity of the Client/Beneficial Owner may be completed during the establishment of a Business Relationship:

a) if this is necessary not to interrupt the normal conduct of business,

b) where there is little risk of money laundering or terrorist financing occurring,

c) where the process of verifying the procedure is completed as soon as practicable after the initial contact.

The basic principles outlined in the Law regarding identification and "Customer Due Diligence" (hereinafter "CDD") measures are the following:

a) Identify and verify the Client identity

b) Identify and take reasonable steps to verify the Beneficial Owner identity and place of residence, including the use of beneficial ownership registers, where available and on a risk-sensitive basis

c) Take reasonable steps to understand the ownership and control structure of the Client, in order to be satisfied that the Client's ownership and control structure is not unduly complex or opaque, or complex or opaque ownership and control structures have a legitimate legal or economic reason

d) Take reasonable steps to assess the purpose of the intended nature of Business Relationship

e) Conduct ongoing monitoring to confirm the information gathered initially.

As a general rule, the Company shall not accept any fund deposits, where the Client/Beneficial Owner has not provided information as to:

i. The full identification of the Client, and

ii. The creation of an economic profile, and/or

iii. The completion of the suitability test, and/or

iv. The completion of the appropriateness test.

f) The Company shall take appropriate measures in order to identify and assess the risks of money laundering terrorist financing activities, before the promotion of any new technology, its services or products.

7.3 Criteria for Accepting New Clients (based on their respective risk) and Client Categorization

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

- *The Categorization of Client risk shall be performed by the AMLCO during the onboarding of the Client and a relevant form shall be completed, signed and stored in each Client's file. The Company does not follow a pre-determined "automatic'' assessment of Client AML risk classification. Albeit the Company maintains a risk based checklist which contains certain risk based criteria to facilitate the risk classification of clients, the ultimate decision regarding the categorization of each Client remains with the AMLCO who categorizes each client according to the criteria mentioned herein and by implementing his professional judgement after reviewing the Client file. In all circumstances the AMLCO's is properly documented.*

7.3.1 *Low Risk Clients*

The Company shall accept Clients who are categorised as low risk Clients as long as the general principles under Sections 8.1, 8.5 and 8.6 are followed.

When assessing the risks of money laundering relating to types of customers, geographic areas, and particular products, services/transactions or delivery channels, the following factors of potentially lower risk situations, as provided by the Law, shall be taken into account.

(1) Customer risk factors:

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

(2) Product, service/transaction or delivery channel risk factors:
a) life insurance policies for which the premium is low;
b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;
d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;
e) products where the risks of money laundering are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money);

(3) Geographical risk factors – registration, establishment, or residence in:
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 consistent with the revised FATF Recommendations and effectively implement those requirements.

The Company may implement simplified due diligence measures with regard to customer if the business relationship or transaction entail lower degree of risk (e.g. for Low Risk Clients) according to Section 8.6 of the Manual.

It is provided that, in the cases mentioned above, the Company has to gather sufficient information to establish if the client relationship entails a lower risk. In this respect, the AMLCO shall be responsible to gather the said information. The said information shall be duly documented and filed, as applicable, according to the record keeping procedures described in Section 11. The Company, in the context of its assessment of the above, pays particular attention to each activity of these customers or any type of transaction that may, by its nature, be regarded as particularly likely to be used for rinsing money laundering or terrorist financing.

7.3.2 *Normal Risk Clients*

The Company shall accept Clients who are categorised as normal risk Clients as long as the general principles under Section 8.1 of the Manual are followed.

Any Client who does not fall under the 'low risk Clients' or 'high risk Clients' categories can be classified as normal risk Client with respect to the Money Laundering risk which the Company faces.

7.3.3 *High Risk Clients*

The Company shall accept Clients who are categorised as high risk Clients as long as the general principles under Section 8.7 of the Manual are followed.

Moreover, the Company shall apply the *Enhanced Client Identification and Due Diligence* measures for high risk Clients, according to Section 8.7 of the Manual and the due diligence and identification procedures for the specific types of high risk Clients mentioned as well in Section 8.8 of the Manual, as applicable.

When assessing the risks of money laundering relating to types of customers, geographic areas, and particular products, services, transactions or delivery channels, the following factors of potentially increasing risk situations, as provided by the Law, shall be taken into account.

(1) Client risk factors:
The following factors may contribute to increasing risk:
a) Clients with income and/or wealth from high-risk sectors such as the extractive industries, construction.
b) Clients about whom credible allegations of wrongdoing have been made.
c) Clients who expect unusually high levels of confidentiality or discretion.
d) Clients whose spending or transactional behaviour makes it difficult to establish 'normal', or expected patterns of behaviour.

e) Very wealthy and influential clients, including clients with a high public profile, non-resident clients and PEPs, or holds another prominent position that might enable them to abuse their position for private gain.
f) The client requests that the firm facilitates the client being provided with a product or service by a third party without a clear business or economic rationale.
g) the business relationship is conducted in unusual circumstances.
h) clients that are resident in geographical areas of higher risk as set out in point (3).
i) legal persons or arrangements that are personal asset-holding vehicles.
j) companies that have nominee shareholders or shares in bearer form or the ownership and control structure is opaque.
k) businesses that are cash-intensive or that are associated with a high risk of financial crime.
l) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business.
m) Client and, in the case of a non-natural person, the beneficial owner of the Client, who is a national of a third country or a Member State and applies for a residence permit or citizenship in the Republic in exchange for the transfer of funds, purchase of property or government bonds, or investments in companies.

(2) Product, service, transaction or delivery channel risk factors:
a) private banking;
b) products or transactions that might favor anonymity;
c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic identification means, relevant trust services as defined in Regulation (EU) No 910/2014 and in the Law concerning the Implementation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant competent Authorities of the Republic;
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;
f) Transactions related to oil, weapons, precious metals, tobacco products, cultural artifacts and other objects of archaeological, historical, cultural and religious significance or of rare scientific value, as well as ivory and protected species.

(3) Geographical risk factors:

Clients established, operating or residing in third-country jurisdictions which have strategic deficiencies in their national AML/CFT regimes which pose significant threats to the financial system of the European Union, as these have been identified by EU Delegated Regulations, as provided in Appendix 4, are by definition of high risk third country jurisdictions considered as High Risk.

Furthermore, the Company shall treat as High Risk Clients, Clients originating, operating or residing in:
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.

(4) Risk Factors based on the Client's behaviour:
(a) Client transactions where there is no apparent legal financial/commercial rationale;
(b) situations where the origin of wealth and/or source of funds cannot be easily verified;
(c) unwillingness of Clients to provide information on the Beneficial Owners of a legal person.

(5) Risk based on the Client's initial communication with the Company:
(a) non face-to-face Client;
(b) Clients introduced by a third person.

Indicatively, the following types of Clients can be classified as high-risk Clients with respect to the Money Laundering risk which the Company faces:

- Clients who are not physically present for identification purposes (non face-to-face Clients);
- Clients whose own shares or those of their parent companies (if any) have been issued in bearer form;
- trust accounts;
- 'Client accounts' in the name of a third person;
- PEPs' accounts;
- Clients who are involved in electronic gaming activities through the internet;
- Clients from high risk third countries;
- cross-frontier correspondent banking relationships with credit institutions-Clients from third countries;
- any other Clients that their nature entail a higher risk of money laundering or terrorist financing;
- any other Client determined by the Company itself to be classified as such.

7.3.4 *Not Acceptable Clients*

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

- Clients who fail or refuse to submit, the requisite data and information for the verification of his identity and the creation of his economic profile, without adequate justification'
- Clients convicted for a Predicate Offence (and are yet to serve their sentence). Depending on the nature of Predicate Offence, is at the Company's discretion not to accept a Client even after having served his/her sentence;
- Clients included in Sanction Lists;
- Shell Banks (Credit institutions and financial institutions are prohibited from entering into, or continuing, a correspondent relationship with a shell bank. It is required that those institutions take appropriate measures to ensure that they do not engage in or continue correspondent relationships with a credit institution or financial institution that is known to allow its accounts to be used by a shell bank);
- Clients who are in the business of arms, defence, military;
- Clients who are in the business of gambling;
- Clients that are unregulated charities;
- Credit institutions, financial organisations and legal persons that operate in the areas of the Republic of Cyprus under Turkish military occupation, which are not incorporated according to the laws of the Republic of Cyprus and do not possess operating license for providing services from CySEC or any other relevant regulatory authority of the Republic of Cyprus, in view of Circular CI144-2008-11.

7.3.5 *Financial inclusion and de-risking*

'De-risking' refers to a decision taken by the Company to no longer offer services to some categories of customers associated with higher ML/TF risk. As the risk associated with individual business relationships will vary, even within one category, the application of a risk-based approach does not require the Company to refuse, or terminate, business relationships with entire categories of customers that are considered to present higher ML/TF risk. The Company shall carefully balance the need for financial inclusion with the need to mitigate ML/TF risk.

As part of this, the Company shall put in place appropriate and risk-sensitive policies and procedures to ensure that its approach to applying CDD measures does not result in unduly denying legitimate customers access to financial services. Where a client has legitimate and credible reasons for being unable to provide traditional forms of identity documentation, the Company shall consider mitigating ML/TF risk in other ways, including by:

- adjusting the level and intensity of monitoring in a way that is commensurate to the ML/TF risk associated with the client, including the risk that a client who may have provided a weaker form of identity documentation may not be who they claim to be; and
- offering only basic financial products and services, which restrict the ability of users to abuse these products and services for financial crime purposes. Such basic products and services may also make it easier for the Company to identify unusual transactions or patterns of transactions, including the unintended use of the product; but it is important that any limits be proportionate and do not unreasonably or unnecessarily limit clients' access to financial products and services.

8 CLIENT DUE DILIGENCE & IDENTIFICATION PROCEDURES

8.1 Client Identification and Due Diligence Procedures

The Company should be 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.

Client Identification and Due Diligence procedures include the following:

i. The identification and the verification of the identity, including electronic identification, on the basis of documents, data or information issued or obtained from a reliable and independent source, including, where available, means of electronic identification, related trust services, as defined in the European Union act "Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC" or any other secure remote or electronic identification process, that is regulated, recognised, approved or accepted by a Supervisory Authority of the Republic.. Creation of an economic profile for the Client/beneficial owner.

ii. The identification of the Client's beneficial owners and legal representative and taking reasonable steps to verify their identity in order to ensure that the Company knows the beneficial owner. With regards to legal persons, trusts, companies, foundations and similar legal arrangements, reasonable steps should be taken to understand the structure of the ownership and customer control. In case of a business relationship with a company or other legal entity or a trust or a similar legal arrangement that is subject to registration requirements of its beneficial owners in relevant Registries, then the firms should collect proof of such registration prior to the establishment of the business relationship. The said proof should bear date of receipt. In the case where the beneficial owner identified is a senior managing official as referred to in subparagraph (ii) of paragraph (a) of the definition of the term "beneficial owner" in Article 2(1) of the Law, the Company shall take the necessary reasonable steps for the verification of the identity of the natural person, who holds the position of senior managing official, and keeps a record to document the actions that were undertaken, as well as any difficulties encountered during the verification process.

iii. The assessment and, where appropriate, the collection of information on the purpose and intended nature of the business relationship.

iv. Continuous supervision of the business relationship by scrutinizing the transactions carried out during that relationship in order to ensure that the transactions carried out are consistent with the data and information held by the person conducting financial or other activity relating to the client, the business and the client's risk profile, and, where appropriate, with regards to the origin of the funds and ensuring that updated documents, data or information are kept.

Provided that when applying the measures of paragraphs (i) and (ii) above, the Company should verify that any third person who intends to act on behalf of the client is duly authorized by the client for that purpose and verify the identity of the third party.

Establishing the nature and purpose of the business relationship

The measures the Company shall take to establish the nature and purpose of the business relationship should be commensurate to the risk associated with the relationship and sufficient to enable the Company to understand who the Client is, and who the Client's beneficial owners are. The Company shall at least take steps to understand:

(a) The nature of the Client's activities or business;
(b) Why the Client has chosen the Company's products and services;
(c) The value and sources of funds that will be flowing through the account;
(d) How the Client will be using the Company's products and services;
(e) Whether the Client has other business relationships with other parts of the Company or its wider group, and the extent to which this affects the Company's understanding of the Client; and
(f) What constitutes 'normal' behaviour for this Client or category of Clients.

The Company shall apply each of the customer due diligence measures and identification procedures as these are set out below, but may determine the extent of such measures depending on the degree of risk taking into consideration at least the following is a non-exhaustive list of risk variables (as provided in Appendix 1 of the AML Law).

The Company must be able to demonstrate to the competent Supervisory Authorities that the extent of the measures is proportionate to the risks of Money Laundering that faces taking into account:

(a) the purpose of an account or relationship;
(b) size of transactions undertaken or the level of assets to be deposited by a customer (as/if applicable);
(c) the regularity or duration of the business relationship.

In this respect, it is the duty of the AMLCO to apply all the relevant Client Due Diligence Identification Procedures described in this Section. Furthermore, the AMLCO shall also be responsible to collect and file the relevant Client identification documents, according to the recording keeping procedures described in Section 11 of the Manual.

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

The identification information and documents be kept by the Company in its records should take the following form:

(a) Original, or
(b) True copy of the original, where the certification is made by the Company itself in cases where it establishes the Client's identity itself, once the original is presented thereto, or
(c) True copy of the original, where the certification is made by third parties provided in Section 8.9 of this Manual, or
(d) True copy of the original, where the certification is made by a competent authority or person that pursuant of the legislation of their countries, is responsible to certify the authenticity of documents or information, in cases where they establish the Client's identity themselves, in which case the documents should be apostilled or notarised format, or
(e) Copy of the original, provided that at least one of the procedures below is followed:
    i. The first payment of the operations is carried out through an account held in the Client's name with a credit institution operating and licensed in a third country, which according to the Advisory Authority's decision, imposes requirements equivalent to those laid down by the EU Directive;
    ii. Obtaining an original or true copy of a direct confirmation of the establishment of a business relationship of a business relationship through direct personal contact, as well as the true name, address, and passport/identity card number of the Client, from a credit

institution or a financial institution, with which the Client cooperates, operating in a Member States or a Third country, Advisory Authority's decision, imposes requirements equivalent to those laid down by the EU Directive;

iii. Contacting the Client via a telephone call at his home or office, on a telephone number verified by an independent and reliable source, during which the Company shall confirm additional aspects of the identity information submitted by the Client during the Client account opening process;

iv. Communicating the Client via a video conference call, provided the video recording and screen shot safeguards apply to such communication;

v. Communicating with the Client through an address that the Company has previously verified from an independent and reliable source, in the form of registered letter e.g. direct mailing of account opening documentation, which the Client shall return to the Company or the sending of security codes required by the Client to access the accounts opened.

(f) Electronic Identify Verification (this method is not currently used by the Company)

Electronic identity verification is carried out either by the Company directly or by a third party, pursuant that both the Company and such third party satisfy the below conditions:

1. The electronic databases kept by the third party or which the third party or the Company has access are registered to and/or approved by the Data Protection Commissioner or the corresponding competent authority in the country the said databases are kept, in order to safeguard personal data;
2. 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 Client's full name, address and date of birth, and negative information such as committing offences as identity theft, inclusion in deceased persons records, inclusion in sanctions and restrictive measures' list by the Council of European Union and the UN Security Council;
3. 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;
4. Transparent procedures have been established allowing the Company to know which information was searched, the result of such search and its significance in relation to the level of assurance as to the Client's identity verification;
5. Procedures have been established allowing the Company to record and save the information used and the result in relation to identity verification.

In addition to the above, the Company evaluates the results of electronic verification in order to be satisfied that proof of identity has been carried out satisfactorily, so that

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 Law, that the customer is actually the person he claims to be.

(Note: Points e. and f. above are not currently used by the Company)

The Company should always be in a position to establish mechanisms for the carrying of quality controls in order to assess the quality of information on which it intends to rely.

The Company should receive information for electronic verification at least from two or more sources and the electronic verification procedure shall at least satisfy the following conditions:

- Identification of the Client's full name and current address from one source, and
- Identification of the Client's full name and either his current address or date of birth from a second source.

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

The documents mentioned above should be accompanied by a true translation should they be in a language other than Greek or English.

The Internal Auditor shall be responsible to review the adequate implementation of all the policies and procedures mentioned in Section 8 of the Manual, at least annually, as per Section 4 of the Manual.

8.2 Time of Application of the Due Diligence and Client Identification Procedures

The Company shall apply Due Diligence and Client Identification Procedures in the following cases:

1. When establishing a business relationship;

   - The identification and verification of the identity of the Client and the Beneficial Owner shall be performed before the establishment of a Business Relationship. In case the Company enters into a new business relationship with a company or other legal entity or with a trust or similar legal arrangement, that is subject to the obligation to record information about its beneficial owner in accordance with the provisions of Article 61A or 61B or 61C of the Law, then the Company must collect proof of registration in the relevant register or an extract of the information relating to the beneficial owner from the relevant register.

   - Nevertheless, in cases where it is necessary not to interrupt the normal conduct of business the process, the verification of the Client and the Beneficial Owner (i.e. collection of the respective supporting documents) may be completed as soon as possible after the initial contact and during the establishment of the business relationship.

2. When carrying out an Occasional Transaction which- (i) amounts to an amount equal to or higher than fifteen thousand euros (€15,000) whether the transaction is carried out in a single operation or in several operations which appear to be linked (as and if ever applicable to the Company);

3. When there is a suspicion of money laundering or terrorist financing, regardless of the amount or any derogation, exemption or minimum threshold pursuant to the provisions of the Law;

4. When there are doubts about the veracity or adequacy of previously obtained customer identification data;
   - If at any time during the Business Relationship, the Company becomes aware that reliable or adequate data and information are missing from the identity and the economic profile of the Client, then the Company takes all necessary action, by applying the Client identification and due diligence procedures according to the Manual, to collect the missing data and information, the soonest possible, so as to identify the Client and update and complete the Client's economic profile.

1. Identification procedures and Client due diligence requirements shall be applied not only to all new Clients but also to existing Clients at appropriate times, depending on the level of risk of being involved in money laundering or terrorist financing (see points 2.- 4. above), or when the Client's relevant circumstances change, or when the Company has a duty, under provisions of the Law, to contact the Client during the relevant calendar year for the purpose of reviewing any material information related to the beneficial owner(s), or if the Company has this duty, according to the provisions of the Law on Administrative Cooperation in the Sector of Taxation.
2.

3. The adequacy of the data and information of the Client's identity and economic profile should also be checked, whenever one of the following events or incidents occurs:

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

   The AMLCO shall:

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

   - **For High Risk Clients Client files should be reviewed for completeness and update once on at least annual basis while for low and normal risk Clients once every two years.**

   The outcome of the said review shall be recorded in a separate note/form which shall be kept in the respective Client file.

8.3 Transactions that Favour Anonymity

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

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

Failure or refusal by a Client to submit, before or during the establishment of a Business Relationship or the execution of an occasional transaction, the requisite data and information for the verification of his identity and the creation of his economic profile (see Section 8.5 of the Manual), without adequate justification, constitutes elements that may lead to the creation of a suspicion that the Client is involved in money laundering or terrorist financing activities. In such an event, the Company shall not proceed with the establishment of the Business Relationship or the execution of the occasional transaction while at the same time the AMLCO considers whether it is justified under the circumstances to submit a report to the Unit, according to point (g) of Section 5.2 of the Manual.

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

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

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

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

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

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

(e) the data and information that are collected before or during the establishment of the Business Relationship, with the aim of constructing the Client's economic profile and, as a minimum, shall include the following:
- the purpose and the reason for requesting the establishment of a Business Relationship
- the anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments
- the Client's size of wealth and annual income and the clear description of the main business/professional activities/operations

(f) the data and information that are used for the construction of the Client-legal person's economic profile shall include, *inter alia*, the following:
- the name of the company
- the country of its incorporation
- the head offices address
- the names and the identification information of the Beneficial Owners
- the names and the identification information of the directors
- the names and the identification information of the authorised signatories
- financial information
- the ownership structure of the group that the Client-legal person may be a part of (country of incorporation of the parent company, subsidiary companies and associate companies, main activities and financial information).

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

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

(h) Client transactions and Client overall activity in general, shall be compared and evaluated against the anticipated account's turnover/activity (as and where applicable), the usual turnover of the activities/operations of the Client and the data and information kept for the Client's economic profile. Significant deviations are investigated and the findings are recorded in the respective Client's file. Transactions that are not justified by the available information on the Client, are thoroughly examined so as to determine whether suspicions over money laundering

or terrorist financing arise for the purposes of submitting an internal report to the AMLCO, according to point (f) of Section 5.2 of the Manual, and then by the latter to the Unit, according to point (g) of Section 5.2 of the Manual. (see also Sections 9. and 10. of this Manual).

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

(a) it is reasonably possible to establish that the Client is the person he claims to be; and
(b) the person who examines the evidence is satisfied, in accordance with the procedures followed under this Law, that the Client is actually the person he claims to be.

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

8.6 Simplified Client Identification and Due Diligence Procedures

The Company may apply simplified customer due diligence measures if they are previously satisfied that the business relationship or transaction has a lower degree of risk, and provided that there is no suspicion of money laundering or terrorist financing activities, provided that the Company adequately monitors the transaction and the business relationship, so that unusual or suspicious transactions can be traced.

With respect to the provisions of the Law and the Directive, the Company may apply simplified Due Diligence Procedures where the Client is categorised as a low risk Client and there is little risk of money laundering. The Company shall not consider however that low risk Client Clients or transactions referred above represent a low risk of money laundering or terrorist financing if there is information available to suggest that the risk of money laundering or terrorist financing may not be low.

It is provided that the Company shall collect sufficient information, so as to decide whether the Client can be exempted according to the provisions - as already mentioned in Section 7.3.1 above. The Company when assessing the abovementioned shall pay special attention to any activity of those Clients or to any type of transactions which may be regarded as particularly likely, by its nature, to be used or abused for money laundering or terrorist financing purposes.

In addition to the above, the Company must exercise continuous monitoring of the business relationships mentioned in Section 7.3.1 according to the provisions of the paragraph (iv) of Section 8.1 or report to the Unit any suspicious transaction or any attempt to carry out a suspicious transaction.

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

8.7.1 General Provisions

The AMLCO shall apply enhanced due diligence measures, in addition to the measures referred to in Sections 8.1, 8.2, 8.3, 8.4 and 8.5, with respect to the Clients categorised as high risk Clients according to the criteria set in Section 7.3.3 of this Manual.

The following EDD measures may be appropriate in high-risk situations:

a. Obtaining and verifying more information about clients than in standard risk situations and reviewing and updating this information both on a regular basis and when prompted by material changes to a client's profile. The Company shall perform reviews on a risk-sensitive basis, reviewing higher risk clients at least annually but more frequently if risk dictates. These procedures may include those for recording any visits to clients' premises, whether at their home or business, including any changes to client profile or other information that may affect Risk Assessment that these visits prompt.
b. Establishing the source of wealth and funds; where the risk is particularly high and/or where the firm has doubts about the legitimate origin of the funds, verifying the source of wealth and funds

may be the only adequate risk mitigation tool. The source of funds or wealth can be verified, by reference to, inter alia:

- an original or certified copy of a recent pay slip;
- written confirmation of annual salary signed by an employer;
- an original or certified copy of contract of sale of, for example, investments or a company;
- written confirmation of sale signed by an advocate or solicitor;
- an original or certified copy of a will or grant of probate;
- written confirmation of inheritance signed by an advocate, solicitor, trustee or executor;
- an internet search of a company registry to confirm the sale of a company.

c. Establishing the destination of funds (where and as applicable).

d. Performing greater levels of scrutiny and due diligence on business relationships than would be typical.

e. Carrying out an independent internal review and, where appropriate, seeking senior management approval of new clients and existing clients on a risk-sensitive basis.

f. Enhanced monitoring of transactions and client relationship on an ongoing basis, including, where necessary, reviewing each transaction as it occurs, to detect unusual or suspicious activity and intensifying the degree and nature of the monitoring of the business relationship in order to determine whether such transactions or activities seem suspicious. This may include measures to determine whether any of the following are out of line with the business risk profile:

- transfers (of cash, investments or other assets);
- the use of wire transfers;
- significant changes in activity;
- transactions involving jurisdictions associated with higher ML/TF risk;
- complex transactions;
- unusually large transactions;
- unusual pattern of transactions;
- transactions that have no apparent economic or lawful purpose.

- Ensuring that the firm is satisfied that a client's use of complex business structures such as trusts and private investment vehicles is for legitimate and genuine purposes, and that the identity of the ultimate beneficial owner is understood.

Below are described due diligence and identification procedures with respect to selected categories of High Risk Clients. It is noted however that the Company, not least because for its operational model, is not expected to interact with the majority of such Clients (with the exception perhaps of Politically Exposed Persons). Therefore the measures set below are provided to be applied as and where needed, as well as for purposes of Compliance with the applicable legislation.

In any case and prior to applying any of the measures set below, the AMLCO and the Company's management shall apply the necessary professional judgement. High Risk Client applications shall be further considered only where the legitimacy and reasonableness of such client's requests to establish a business relationship and receive the Company's services is ascertained.

8.7.2 Trust accounts

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

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

verify the identity of all Beneficial Owners of the Trust, according to the Client identification procedures prescribed in throughout Section 8 of this Manual. It is clarified that Beneficial Owners in the case of trusts include:

- the settlor;
- the trustee or commissioner;
- the protector, if any;
- 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;
- any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means.

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

8.7.3 Non face-to-face Clients

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

1. Whenever a Client 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 Client, especially a non-resident of the Republic, requests the establishment of a Business Relationship or an Occasional Transaction (if ever applicable) through mail, telephone, or the internet without presenting himself for a personal interview, the Company must follow the established Client identification and due diligence procedures, as applied for Clients with whom it comes in direct and personal contact and obtain exactly the same identification information and documents, as required by the Law and the Directive, depending on the type of the Client.

   Further to the supplementary measures to verify supplied documents of a Client, who has not been physically present for identification purposes, the Company may utilize the below practical procedures for obtaining additional documents, data or information for the verification of a Client's identity:

   i. The first payment of the operations is carried out through an account held in the Client's name with a credit institution operating and licensed in a third country, which according to the Advisory Authority's decision, imposes requirements equivalent to those laid down by the EU Directive.
   ii. Obtaining an original or true copy of a direct confirmation of the establishment of a business relationship of a business relationship through direct personal contact, as well as the true name, address, and passport/identity card number of the Client, from a credit institution or a financial institution, with which the Client cooperates, operating in a Member States or a Third country, Advisory Authority's decision, imposes requirements equivalent to those laid down by the EU Directive.
   iii. Contacting the Client via a telephone call at his home or office, on a telephone number verified by an independent and reliable source, during which the Company shall confirm additional aspects of the identity information submitted by the Client during the Client account opening process.
   iv. Communicating the Client via a video conference call, provided the video recording and screen shot safeguards apply to such communication.

   It is provided that a Client, whose identity was verified hereunder cannot deposit (if ever applicable to the Company) an amount over €2,000 per annum, if ever that would be applicable to the Company, irrespective of the number of accounts that he/she keeps with the Company, unless the Company, for the verification of the Client's identity takes an additional measure, as per this paragraph;

Further to the above, the Company shall apply appropriate measures and procedures in order to:

1. Confirm and monitor both the amount of the Client's deposit and the risk for money laundering or terrorist financing, as well as to take additional measures to verify the Client's identity depending on the degree of the risk;
2. Ensure the normal conduct of business is not interrupted where the amount of the Client's deposit exceeds the amount of €2,000 annually;
3. Warn the Client appropriately and in due time for the above mentioned procedure in order to obtain the Client's express consent, prior to its commencement

v. Communicating with the Client through at an address that the Company has previously verified from an independent and reliable source, in the form of registered letter e.g. direct mailing of account opening documentation, which the Client shall return to the Company or the sending of security codes required by the Client to access the accounts opened.

8.7.4 Account in 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 Section 8.8.6, all the following supplementary due diligence measures:

1. the Company takes physical custody of the bearer share certificates while the Business Relationship is maintained or obtains a confirmation from a bank operating in the Republic or a country of the EEA that it has under its own custody the bearer share certificates and, in case of transferring their ownership to another person, shall inform the Company accordingly;
2. the account is closely monitored throughout its operation. At least once a year, a review of the accounts' transactions and turnover is carried out and a note is prepared summarising the results of the review which shall be kept in the Client's file;
3. if the opening of the account has been recommended by a third person as defined in Section 8.9., at least once every year, the third person who has introduced the Client provides a written confirmation that the capital base and the shareholding structure of the company-Client or that of its holding company (if any) has not been altered by the issue of new bearer shares or the cancellation of existing ones. If the account has been opened directly by the company-Client, then the written confirmation is provided by the company-Client's directors
4. when here is a change to the Beneficial Owners, the Company examines whether or not to permit the continuance of the account's operation.

8.7.5 Clients from countries which inadequately apply FATF's recommendations, EU non-cooperative tax jurisdictions or High Risk Third Countries

The FATF 40+9 Recommendations and the EU Commission constitute the primary internationally recognised standards for the prevention and detection of Money Laundering and Terrorist Financing. The Company shall consider as high-risk jurisdictions

- Third-country jurisdictions which have strategic deficiencies in their national AML/CFT regimes which pose significant threats to the financial system of the European Union (see also Appendix 4);
- Clients from countries which inadequately apply FATF's recommendations **-** the FATF High-risk and other monitored jurisdictions are available at http://www.fatf-gafi.org/countries/#high-risk.

Further to the above, the AMLCO shall consider as high risk third country any other jurisdictions identified during his review of relevant information such as 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 (https://www.coe.int/en/web/moneyval/)] and the International Monetary Fund

(https://www.imf.org/external/index.htm) and other organizations mentioned in Section 6.4 of the Manual.

For Client relationships with high risk third country jurisdictions, the Company shall apply a combination or all of the below measures, as deemed necessary and appropriate in each case:

1. Increasing the quantity of information obtained for Client Due Diligence purposes:
    - Information about the client's and/or beneficial owner's identity, or the client's ownership and control structure, to be satisfied that the risk associated with the relationship is well understood.

      This may include obtaining and assessing information about the client's and/or beneficial owner's reputation and assessing any negative allegations against the client and/or beneficial owner. Examples include:

        i. information about family members and close business partners;

        ii. information about the client's or beneficial owner's past and present business activities; and

        iii. adverse media searches.

    - Information about the intended nature of the business relationship to ascertain that the nature and purpose of the business relationship is legitimate and to help firms to obtain a more complete client risk profile.

      This may include obtaining information on:

      a. the number, size and frequency of transactions that are likely to pass through the account, to enable the firm to spot deviations that might give rise to suspicion (in some cases, requesting evidence may be appropriate), as well as the purpose of the transactions planned or executed;;

      b. why the client is looking for a specific product or service, in particular where it is unclear why the client's needs cannot be met better in another way, or in a different jurisdiction;

      c. the destination of funds;

      d. the nature of the client's or beneficial owner's business, to enable the firm to better understand the likely nature of the business relationship.

2. Increasing the quality of information obtained for Client Due Diligence purposes to confirm the client's or beneficial owner's identity including by:
    - requiring the first payment to be carried out through an account verifiably in the client's name with a bank subject to CDD standards that are not less robust than those set out in Chapter II of AML IV Directive (if and as applicable); or
    - establishing that the client's and/or beneficial owner's wealth and the funds that are used in the business relationship are not the proceeds of criminal activity and that the source of wealth and source of funds are consistent with the firm's knowledge of the client and/or beneficial owner and the nature of the business relationship. In some cases, where the risk associated with the relationship is particularly high, verifying the source of wealth and the source of funds may be the only adequate risk mitigation tool. The source of funds or wealth can be verified, inter alia, by reference to VAT and income tax returns, copies of audited accounts, pay slips, public deeds or independent media reports. (note

3. Increasing the number and frequency of reviews to be satisfied that the firm continues to be able to manage the risk associated with the individual business relationship or conclude that the relationship no longer corresponds to the firm's risk appetite and to help identify any transactions that require further review, including by:
    - increasing the number and frequency of reviews of the business relationship to ascertain whether the client's risk profile has changed and whether the risk remains manageable;

- obtaining the approval of senior management to commence or continue the business relationship to ensure that senior management are aware of the risk their firm is exposed to and can take an informed decision about the extent to which they are equipped to manage that risk;
- reviewing the business relationship on a more regular basis to ensure any changes to the client's risk profile are identified, assessed and, where necessary, acted upon; or
- conducting more frequent or in-depth transaction monitoring to identify any unusual or unexpected transactions that might give rise to suspicion of ML/TF. This may include establishing the destination of funds or ascertaining the reason for certain transactions, and the selection of transactions that need further examination .

Transactions for which there is no obvious economic benefit or legitimate purpose, are further investigated for the purpose of documenting financial, commercial or investment incentives for transactions. If the Obligatory Entity does not get sufficient information or explanations to the full satisfaction of the legality of a transaction submit, through the compliance officer, a disclosure report to the Unit.

8.8 Client Identification and Due Diligence Procedures (Specific Cases)

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

8.8.1 Natural persons residing in the Republic

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

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

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

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

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

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

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

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

8.8.2 Natural persons not residing in the Republic

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

2. In addition to the information collected according to Section directly above (persons residing in the Republic), without prejudice to the application on a risk-sensitive basis, the Company shall require and receive information on public positions which the prospective Client holds or held in the last twelve (12) months as well as whether he is a close relative or associate of such individual, in order to verify if the Client is a PEP.

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

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

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

8.8.3 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 Sections 8.8.1 and 8.8.2 above.

8.8.4 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 shall obtain a list of the members of board of directors/management committee of the abovementioned organisations and verifies the identity of all individuals that have been authorised to manage the account according to the procedures set in Sections 8.8.1 and 8.8.2.

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

1. In the case of unincorporated businesses, partnerships and other persons with no legal substance, the identity of the directors, partners, Beneficial Owners and other individuals who are authorised to manage the account shall be verified according to the procedures set in Sections 8.8.1 and 8.8.2.

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

2. The Company shall obtain documentary evidence of the head office address of the business, ascertains the nature and size of its activities and receives all the information required according to Section 8.5 for the creation of the economic profile of the business.

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

8.8.6 Accounts of legal persons

1. For Clients that are legal persons, the Company shall establish that the natural person appearing to act on their behalf, is appropriately authorised to do so and his identity is established and verified according to the procedures set in Sections 8.8.1 and 8.8.2.

2. The Company shall take all necessary measures for the full ascertainment of the legal person's control and ownership structure as well as *the verification of the identity of the natural persons* who are the Beneficial Owners and exercise control over the legal person according to the procedures set in Sections 8.8.1 and 8.8.2.

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

   (a) the registered number
   (b) the registered corporate name and trading name used
   (c) the full addresses of the registered office and the head offices
   (d) the telephone numbers, fax numbers and e-mail address
   (e) the members of the board of directors
   (f) the individuals that are duly authorised to operate the account and to act on behalf of the legal person
   (g) the Beneficial Owners of private companies and public companies that are not listed in a regulated market of an EEA country or a third country which is assessed by the Company as lower AML risk taking into consideration the Risk Factor Guidelines and Annex II of the Law.
   (h) the registered shareholders that act as nominees of the Beneficial Owners
   (i) the economic profile of the legal person, according to the provisions of Section 8.5.

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

   (a) certificate of incorporation and certificate of good standing (where available) of the legal person
   (b) certificate of registered office
   (c) certificate of directors and secretary
   (d) certificate of registered shareholders in the case of private companies and public companies that are not listed in a regulated market of a third country which is assessed by the Company as lower AML risk taking into consideration the Risk Factor Guidelines and Annex II of the Law

(e) memorandum and articles of association of the legal person
(f) a resolution of the board of directors of the legal person for the opening of the account and granting authority to those who will operate it
(g) in the cases where the registered shareholders act as nominees of the Beneficial Owners, a copy of the trust deed/agreement concluded between the nominee shareholder and the Beneficial Owner, by virtue of which the registration of the shares on the nominee shareholder's name on behalf of the Beneficial Owner has been agreed
(h) documents and data for the verification, according to the procedures set in Sections 8.8.1 and 8.8.2, of the identity of the persons that are authorised by the legal person to operate the account, as well as the registered shareholders and Beneficial Owners of the legal person.

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

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

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

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

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

9. Apart from verifying the identity of the Beneficial Owners, the Company shall identify the persons who have the ultimate control over the legal person's business and assets. In the cases that the ultimate control rests with the persons who have the power to manage the funds, accounts or investments of the legal person without requiring authorisation and who would be in a position to override the internal procedures of the legal person, the Company, shall verify the identity of the natural persons who exercise ultimate control as described above even if those persons have no direct or indirect interest or an interest of less than 25% +1 share in the legal person's ordinary share capital or voting rights.

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

    (a) the Company shall ascertain the legal substance, the name and the date of establishment of the trust and verify the identity of the trustor, trustee and Beneficial Owners, according to the procedures set in Sections 8.8.1 and 8.8.2
    (b) furthermore, the Company shall ascertain the nature of activities and the purpose of establishment of the trust as well as the source and origin of funds requesting the relevant extracts from the trust deed and any other relevant information from the trustees. All relevant data and information should be recorded and kept in the Client's file.

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

1. The Company shall establish and maintain Business Relationships or execute Occasional Transactions with persons who carry out the above services and activities which are incorporated and/or operating in a third country which is assessed by the Company as lower AML risk taking into consideration the Risk Factor Guidelines and Annex II of the Law, provided that the said persons:

    (a) possess the necessary license or authorisation from a competent supervisory/regulatory authority of the country of their incorporation and operation to provide the said services, and
    (b) are subject to supervision for the prevention of Money Laundering purposes.

2. In the case of the establishment of a Business Relationship or the execution of an Occasional Transaction with persons who carry out the above services and activities and which are incorporated and/or operating in a third country other than those mentioned in point (1) above, the Company shall request and obtain, in addition to the abovementioned, in previous points, documentation and the information required by the Manual for the identification and verification of persons, including the Beneficial Owners, the following:

    (a) a copy of the license or authorisation granted to the said person from a competent supervisory/regulatory authority of its country of incorporation and operation, whose authenticity should be verified either directly with the relevant supervisory/regulatory authority or from other Independent and Reliable Sources, and
    (b) adequate documentation and sufficient information in order to fully understand the control structure and management of the business activities as well as the nature of the services and activities provided by the Client.

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

4. In particular, the following client due diligence measures should be followed in case of funds:

i. Risk categorize the fund taking into consideration the following factors:

- Regulated/unregulated fund
- EU fund/non-EU fund/Third country equivalent/high-risk third country
- Listed in a reputable stock exchange
- Complex structure
- Type of investors
- Type of investments

- Size of the fund

ii. Establish the type of legal entity and obtain relevant governing documents:

iii. Depending on whether the fund is regulated or not, where it is geographically registered and its overall risk, apply the appropriate client due diligence measures (SDD/EDD) to the following natural or legal persons (including outsourced providers and delegates):

- Fund manager
- Investment advisor
- Fund administrator
- Investment manager
- Custodians
- Holders of management shares
- Depository
- Underlying investors
- Distributors

iv. Information on the fund by ascertaining the purpose/objective of operation and verification of the legitimacy thereof (e.g., constitutional documents, offering memorandum, prospectus, KIID and similar documentation)

v. Information on investors including country of origin, type of investor (e.g. professional) and where considered necessary, the identification of the investors as part of the EDD measures

vi. Information on the investments (type, location, origin etc)

Fund documentation

A. For the Fund, obtain:

I. Fund Documents

1. Constitutional documents, certificates of incorporation
2. Offering memorandum,
3. Prospectus
4. KIID and similar documentation

II. Documents to collect and retain where applicable:

1. Valid license or authorisation from a competent authority from the country of its incorporation, operation validated by the Members from fund's regulator website
2. Identification documents for all relevant parties
3. Audited financial statements or other equivalent financial disclosures
4. Prospectus of fund (or equivalent document)
5. Information collected from regulator's website
6. Evidence of background screening searches considering any negative media
7. Internal risk assessment
8. Evidence of management approvals, if applicable

B. For the Fund Manager:

I. Natural Person(s):

Refer to the relevant section of this Manual.

II. Legal Person(s):

Refer to the relevant section of this Manual.

C. For the Investors:

I. Letter signed by the Fund Manager indicating:

1. the names of the Investors
2. percentages of interest each Investor holds in the Fund and
3. confirmation that the Fund Manager(s) has conducted the necessary due diligence procedures on all Investors in accordance with the Anti Money Laundering procedures of FATF or any organization member of FATF.

II. For the Investors (Natural Persons) holding directly or indirectly more than 25% interest in the Company - Refer to the relevant section of this Manual.

8.8.8 Nominees or agents of third persons

1. The Company shall take reasonable measures to obtain adequate documents, data or information for the purpose of establishing and verifying the identity, according to the procedures set in Sections 8.8.1 and 8.8.2 of the Manual:

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

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

8.8.9 Politically Exposed Persons "PEP" accounts

The Company shall apply the following with respect to the accounts of "Politically Exposed Persons" as well as to accounts of their close family members and business associates:

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

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

2. In order to effectively manage such risks, the Company shall assess the countries of origin of its Clients in order to identify the ones that are more vulnerable to corruption or other third country high risks jurisdictions, as per Section 8.7.5.

   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 shall retrieve information from the country assessment reports prepared by the FATF or other regional bodies operating in accordance with FATF's principles (e.g. Moneyval Committee of the Council of Europe) or the International Monetary Fund.

3. Without prejudice to the application, on a risk-sensitive basis, of enhanced Client due diligence measures (Section 8.8.1 of the Manual), where a person has ceased to be entrusted with a prominent public function within the meaning of point (4) below for a period of at least one year, the Company shall not be obliged to consider such a person as politically exposed.

4. The Company adopts the following additional due diligence measures when it establishes a Business Relationship or carry out an Occasional Transaction with a PEP:

   (a) the Company puts in place appropriate risk management procedures to enable it to determine whether a prospective Client is a PEP. Such procedures may include, depending on the degree of risk, the acquisition and installation of a reliable commercial electronic database for PEPs, seeking and obtaining information from the Client himself or from publicly available information. In the case of legal entities and arrangements, the procedures will aim at verifying whether the Beneficial Owners, authorised signatories and persons authorised to act on behalf of the legal entities and arrangements constitute PEPs. In case of identifying one of the above as a PEP, then automatically the account of the legal entity or arrangement should be subject to the relevant procedures specified in this Section of the Manual;
   (b) the decision for establishing a Business Relationship or the execution of an Occasional Transaction with a PEP is taken by a member of the Senior Management of the Company and the decision is then forwarded to the AMLCO. When considering whether to approve a PEP relationship, senior management should base their decision on the level of ML/TF risk the firm would be exposed to if it entered into that business relationship and how well equipped the firm is to manage that risk effectively. When establishing a Business Relationship with a Client (natural or legal person) and subsequently it is ascertained that the persons involved are or have become PEPs, then an approval is given for continuing the operation of the Business Relationship by an *Executive Director* of the Company which is then forwarded to the AMLCO;
   (c) before establishing a Business Relationship or executing an Occasional Transaction with a PEP, the Company shall obtain adequate documentation to ascertain not only the identity of the said person but also to assess his business reputation (e.g. reference letters from third parties);
   (d) the Company shall create the economic profile of the Client by obtaining the information specified in Section 8.5. The details of the expected business and nature of activities of the Client forms the basis for the future monitoring of the account. The profile shall be regularly reviewed and updated with new data and information. The Company shall be particularly cautious and most vigilant where its Clients are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, cigarettes and alcoholic drinks;
   (e) the Company shall review the information holds about the PEP to ensure that any new or emerging information that could affect the Risk Assessment is identified in a timely fashion. The frequency of ongoing monitoring should be determined by the level of high risk associated with the relationship;
   (f) the account shall be subject to (at least) annual review in order to determine whether to allow its continuance of operation. A short report shall be prepared summarising the results of the review by the person who is in charge of monitoring the account. The report shall be submitted for consideration and approval to the Board and filed in the Client's personal file.

8.8.10 Identifying the Client's senior managing officials

Where the Client is a legal entity, the Company shall make every effort to identify the beneficial owner. The Company shall resort to identifying the Client's senior managing officials as beneficial owners only if:

a) it has exhausted all possible means of identifying the natural person who ultimately owns or controls the Client;

b) its inability to identify the natural person who ultimately owns or controls the Client does not give rise to suspicions of ML/TF; and

c) it is satisfied that the reason given by the Client as to why the natural person who ultimately owns or controls the Client cannot be identified is plausible.

When deciding which senior managing official, or which senior managing officials, to identify as beneficial owner, the Company shall consider who has ultimate and overall responsibility for the Client and takes binding decisions on the Client's behalf. In those cases, the Company shall clearly document its reasons for identifying the senior manager, rather than the Client's beneficial owner, and must keep records of their actions.

8.8.11 Identifying the beneficial owner of a public administration or a state-owned enterprise

Where the Client is a public administration or a state-owned enterprise, the Company shall follow the guidance in Section 8.8.10 of the Manual to identify the senior managing official. In those cases, and in particular where the risk associated with the relationship is increased, for example because the state-owned enterprise is from a country associated with high levels of corruption, the Company shall take risk-sensitive steps to establish that the person they have identified as the beneficial owner is properly authorised by the Client to act on the Client's behalf.

The Company shall also have due regard to the possibility that the senior managing official of the Client may be a PEP. Should this be the case, the Company must apply EDD measures to that senior managing official in line with Section 8.8.9 of the Manual, and assess whether the extent to which the PEP can influence the Client gives rise to increased ML/TF risk and whether it may be necessary to apply EDD measures to the Client.

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

1. The Company may rely on third persons for the identifying the customer and verifying the customer's and its ultimate beneficial owner's identity on the basis of documents, data or information obtained from reliable and independent source and obtaining information on the purpose and intended nature of the business relationship; (i.e. for points (a), (b) and (c) of Section 61.1 of the Law Client identification and due diligence procedures), provided that:

   (a) the third person *makes immediately available* all data and information, which must be certified true copies of the originals or as otherwise acceptable by current CySEC practices, that were collected in the course of applying Client identification and due diligence procedures and provides these directly to the Company.
   (b) the Company applies the appropriate due diligence measures on the third person with respect to his professional registration and procedures and measures applied from the third person for the prevention of Money Laundering and Terrorist Financing, according to the provisions of the Directive.
   (c) The Company applies appropriate measures to ensure that the third person transmits immediately the appropriate identification and verification copies of the customer's identity, including, if available, data obtained by means of electronic identification, with relevant trust services, as defined in Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market or any other secure remote or electronic

identification process, that is regulated, recognised, approved or accepted by a Supervisory Authority of the Republic.

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

2. Subject to the third party being:
   a. a credit or financial institution which is an authorised entity in accordance with the competent law of its country of incorporation and/or operation as well as supervision for the purposes of compliance with the measures for the prevention of ML & TF;
   b. an auditor, external accountant, insolvency practitioner, tax adviser, notary or other independent legal professional who is regulated by a professional body specified in the regulations in accordance with the competent law of its country of incorporation and/or operation as well as supervision for the purposes of compliance with the measures for the prevention of ML & TF;
   c. equivalent persons, in EEA and non-EEA states, to these two categories who are subject to mandatory professional registration and supervised for money laundering compliance in terms of the directive or an equivalent manner;

   provided that such third party applies due diligence measures to their clients and record keeping procedures which are in compliance with the EU Directive, and which are subject to supervision which complies with the requirements of the EU Directive.

3. Obliged entities are prohibited from relying on third parties established in high-risk third countries. However, each competent Supervisory Authority may exclude from this prohibition branches and subsidiaries of a majority holding of obligated entities established in the European Union where such branches and subsidiaries fully comply with the policies and procedures applicable at group level in accordance with Article 68A of the Law.

4. The Company receives data and information to verify that the third party is subject to professional registration under relevant law or other regulation in the country of its establishment and / or operation, and for purposes of supervision compliance with measures to prevent money laundering or financing of terrorism.

5. Further to point 2 and 3 above, the Company, before accepting the Client identification data verified by the said third person, shall apply the following additional measures/procedures:

   (a) the AMLCO or the appointed person shall assess and evaluate, according to point (m) of Section 5.2 of this Manual, the systems and procedures applied by the third person for the prevention of Money Laundering and Terrorist Financing, as applicable;
   (b) the Company concludes an agreement with the third party providing the obligations of each party;
   (c) the AMLCO shall maintain a separate file for every third person of the present paragraph, where it stores the assessment report of point (a) and other relevant information;
   (d) the commencement of the cooperation with the third person and the acceptance of Client identification data verified by the third person is subject to approval by the AMLCO, according to point (m) of Section 5.2 of the Manual.

6. The Company may rely on third persons only at the outset of establishing a Business Relationship or the execution of an Occasional Transaction for the purpose of verifying the identity of their Clients. According to the degree of risk any additional data and information for the purpose of updating the Client's economic profile or for the purpose of examining unusual transactions executed through the account, is obtained from the natural persons (directors, Beneficial Owners) who control and manage the activities of the Client and have the ultimate responsibility of decision making as regards to the management of funds and assets.

It is provided that, the ultimate responsibility for meeting the above-mentioned measures and procedures shall remain with the Company.

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

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

9 ON-GOING MONITORING PROCESS

9.1 General

The constant monitoring of the Clients' activity and transactions is an imperative element in the effective controlling of the risk of Money Laundering.

The Company is required to have a full understanding of normal and reasonable (account) activity of its Clients and their economic profile, so that it is able to identify transactions or other Client activity which fall outside the regular pattern or other complex or unusual transactions or transactions without obvious economic purpose or clear legitimate reason. Without such knowledge, the Company shall not be able to discharge its legal obligation to identify and report suspicious transactions to the Unit, according to point (g) of Section 5.2 and Section 10 of the Manual.

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

9.2 Procedures

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

(a) the identification of:
- all high risk Clients, as applicable; the Company shall be able to produce detailed lists of high risk Clients, so as to facilitate enhanced monitoring of accounts and transactions, as deemed necessary;
- transactions which, as of their nature, may be associated with money laundering or terrorist financing;
- unusual or suspicious transactions that are inconsistent with the economic profile of the Client for the purposes of further investigation;
- in case of any unusual or suspicious transactions, the head of the department providing the relevant service or any other person who identified the unusual or suspicious transactions shall be responsible to communicate with the AMLCO.

(b) further to point (a) above, the investigation of unusual or suspicious transactions by the AMLCO. The results of the investigations are recorded in a separate memo and kept in the file of the Clients concerned.

(c) the ascertainment of the source and origin of the funds credited to Client's accounts under advice (to the extent deemed necessary.

(d) the use of appropriate and proportionate IT systems, where deemed necessary, including:
- adequate automated electronic management information systems which will be capable of supplying the Board of Directors and the AMLCO, on a timely basis, all the valid and necessary information for the identification, analysis and effective monitoring of Client accounts and transactions based on the assessed risk for money laundering or terrorist financing purposes, in view of the nature, scale and complexity of the Company's business;

- automated electronic management information systems to extract data and information that is missing regarding the Client identification and the construction of a Client's economic profile.

(e) the use of thresholds, and an appropriate review process by which unusual behaviours are promptly reviewed by relationship management staff or (at certain thresholds) the compliance functions or senior management.

(f) the monitoring of Client activity and transactions for any indication of suspicious transactions, (see also Section 10.3 of this Manual for more details).

(g) Monitoring public reports or other sources of intelligence to identify information that relates to clients or to their known associates, businesses to which they are connected, potential corporate acquisition targets or third party beneficiaries to whom the client makes payments.

(h) the on-going monitoring of the business relationship in order to determine whether there are reasonable grounds to suspect that Client accounts contain proceeds derived from serious tax offences.

10 SUSPICIOUS TRANSACTIONS/ACTIVITIES – RECOGNITION & REPORTING TO THE UNIT

10.1 Registration for submission of Suspicious Transactions/Activities to the Unit

The Company registered with the goAML IT System in order for the submission of suspicious transactions/activities to the Unit to be performed in accordance to the provisions of CySEC's Circular C058 and the Directive issued by the Unit relating to the amended procedures followed for the submission of suspicious transactions/activities to the Unit.

10.2 Reporting of Suspicious Transactions to the Unit

The Company, in cases where there is an attempt of executing transactions (if and as applicable) which knows or suspects that are related to money laundering or terrorist financing, reports, through the AMLCO its suspicion to the Unit shall be in accordance with point (g) of Section 5.2 and this Section 9 of the Manual.

10.3 Suspicious Transactions/ Monitoring of Suspicious Transactions

1. The definition of a suspicious transaction as well as the types of suspicious transactions which may be used for Money Laundering are almost unlimited. A suspicious transaction will often be one which is inconsistent with a Client's known, legitimate business or personal activities or with the normal business of the specific account, or in general with the economic profile that the Company has created for the Client. The Company shall ensure that it maintains adequate information and knows enough about its Clients' activities in order to recognise on time that a transaction or a series of transactions or activities which is unusual or suspicious.

2. Examples of what might constitute suspicious transactions/activities related to Money Laundering are listed in Appendix 3 of the Manual. The relevant list is not exhaustive nor it includes all types of transactions that may be used, nevertheless it can assist the Company and its employees (especially the AMLCO) in recognising the main methods used for Money Laundering and Terrorist Financing. The detection by the Company of any of the transactions contained in the said list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds, the nature and economic/business purpose of the underlying transaction, and the circumstances surrounding the particular activity.

3. In order to identify suspicious Client activities the AMLCO shall perform the following activities throughout the Client relationship:
   - understand the economic profile, including the level and source of funds of the client and the business activities of the Client so that they are able to detect any client behaviour not consistent with its profile;

- remain vigilant in relation to Client requests for advice indicating that the Client might be attempting to disguise the origin or ownership of funds or assets or otherwise perform money laundering;
- monitor on a continuous basis any changes in the Client's financial status, business activities, type of transactions etc. (i.e. any changes which are not consistent with the economic profile that the Company has formed about the Client);
- monitor on a continuous basis if any Client is engaged in any of the practices described in the list containing examples of what might constitute suspicious transactions/activities related to Money Laundering which is mentioned in Appendix 3 of this Manual.

Furthermore, the AMLCO shall perform the following activities:

- receive and investigate information from the Company's employees, on suspicious transactions which creates the belief or suspicion of money laundering. This information is reported on the Internal Suspicion Report. The said reports are archived by the AMLCO;
- evaluate and check the information received from the employees of the Company, with reference to other available sources of information and the exchanging of information in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained on the report which is submitted to the AMLCO is evaluated on the Internal Evaluation Report, which is also filed in a relevant file;
- if, as a result of the evaluation described above, the AMLCO decides to disclose this information to the Unit, then he prepares a written report, which he submits to the Unit, according to point (g) of Section 5.2 and Section 10.4 below;
- if as a result of the evaluation described above, the AMLCO decides not to disclose the relevant information to the Unit, then he fully explains the reasons for his decision on the Internal Evaluation Report.

10.4 AMLCO's Report to the Unit

According to Circular C058, all the reports of the AMLCO of point (g) of Section 5.2 of the Manual shall be submitted to the Unit through the **goAML Professional Edition (PE)**", by the completion of the online report on the web-application of the UNIT or by the completion of the relevant XML Report.

After the submission of a suspicious report of point (g) of Section 5.2 of the Manual, the Company may subsequently wish to terminate its relationship with the Client concerned for risk avoidance reasons. In such an event, the Company exercises particular caution, according to Section 48 of the Law, not to alert the Client concerned that a suspicious report has been submitted to the Unit. Close liaison with the Unit is, therefore, maintained in an effort to avoid any frustration to the investigations conducted.

After submitting the suspicious report of point (g) of Section 5.2 of the Manual, the Company adheres to any instructions given by the Unit and, in particular, as to whether or not to continue or suspend a particular transaction or to maintain the particular account active.

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

Furthermore, after the submission of a suspicious report of point (g) of Section 5.2 of the Manual, the Clients' accounts concerned as well as any other connected accounts are placed under the close monitoring of the AMLCO.

10.5 Submission of Information to the Unit

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

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

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

The Company, its directors and employees are not allowed to disclose to the customer or third parties the fact that information on suspicious transactions is transmitted, transmitted or transmitted to the Unit in accordance with Article 69 of the Law or that there is or that an analysis of such information or suspicious transactions can be carried out in relation to money laundering or terrorist financing.

The Company shall legally protect any employees and representatives of the Company who submit an internal report or report to the Unit for suspicious transactions, pursuant to the provisions of Article 69 of the Law, against any exposure to threats, retaliation, or hostile action and in particular by adverse acts or discrimination in the workplace. A person who is exposed to threats or hostile action or adverse or discriminatory employment actions due to the fact that he submitted a suspicious transaction report or a suspicious activity report has the right to file a complaint with CySEC as well as the right to effective remedy.

It is essential to note that in all cases where a person knows or suspects that another person is engaged in money laundering or terrorist financing and the information or other matter on which that knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment, there is an obligation to disclose the information or other matter to the Unit as soon as is reasonably practicable after it comes to his attention.

Failure to make such a disclosure is a serious criminal offence punishable with up to 2 years imprisonment and/or a criminal fine not exceeding €5,000 as per section 27(4) of the Law (See section 1.5.5). Therefore, it is never appropriate to delay making a disclosure to MOKAS pending an application to the court for directions. Firms must report the matter to the Unit as soon as reasonably practicable.

In addition, firms should refrain from carrying out transactions which they know or suspect to be related with money laundering or terrorist financing, before they inform the Unit. If it is considered impossible to refrain from carrying out the transaction or is likely to disturb efforts of an operation to track suspects of money laundering or terrorist financing, the Company must inform the Unit immediately afterwards.

11 RECORD-KEEPING PROCEDURES

11.1 General

According to the Law, records for the following documents should be kept for a period of 5 years after the completion of the Business Relationship, or the execution of the last transaction (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):

- Copies of the evidential material of the Client required for compliance with the due diligence requirements
- Relevant evidential material and details of all business relations and transactions, including documents for recording transactions in the accounting books
- Correspondence with the client

It is provided that the documents/data mentioned above, which may be relevant to ongoing investigations shall be kept by the Company until the Unit or CySEC or the Tax Authorities – as applicable – confirm that the investigation has been completed and the case has been closed.

11.2 Format of Records

The Head of Back Office Department of the Company shall retain the documents/data mentioned in Section 11.1 of the Manual, other than the original documents or their Certified true copies that are kept in a hard copy form, in other forms, such as electronic form, provided that the Head of Back Office Department shall be able to retrieve the relevant documents/data without undue delay and present them at any time, to CySEC or to the Unit, after a relevant request.

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

11.3 Certification & Language of Documentation

(a) The documents/data obtained, shall be in their original form or in a certified true copy form. In the case that the documents/data are certified as true by a different person than the Company itself or by the third person mentioned in Section 8.9, the documents/data must be apostilled or notarised.
(b) A true translation shall be attached in the case that the documents of point (1) above are in a language other than Greek of English.

Each time the Company shall proceed with the acceptance of a new Client, the Head of Back Office Department shall be responsible for ensuring compliance with the provisions of points 1 and 2 above as well as the provisions of the Company's Client Acceptance Policy and the Acceptable certification Standards therein. According to the Company's Client Acceptance policies and related compliance procedures, Clients should provide the Company with either Original documents or Notarised/Certified True Copies of the Originals.

The AMLCO shall ensure that the said policy shall take into consideration the requirements of the Law and the Directive.
The Internal Auditor shall review the adherence of the Company to the above, at least annually.

11.4 Beneficial Owner's Register

The Finance and Accounting Department of the Company shall maintain accurate and up-to-date information on the Company's beneficial owners, including the details of the rights held by the beneficial owners.

The beneficial owners, including beneficial owners through shares, voting rights, property rights, bearer shares or control by other means, provide to the Company all the information necessary to comply with requirements provided for above.

in addition to the information on the legal beneficiary, the Company's Finance and Accounting Department shall provide information on the beneficial owner(s), when the Company undertakes due diligence action and relevant identification procedures, as defined in the AML Law.

The competent Supervisory Authority, the Unit, the Customs and Excise Department, the Department of Taxation and the Police, in the context of exercising their responsibilities, may have access to the information referred to above.

The information referred to above shall be recorded in a centralised Beneficial Owner Register of Express Trusts and similar legal arrangements. The Register is compiled, kept and published by the Registrar of Companies and Official Receiver, who, as the authority responsible for keeping the Register, stores information about companies and others legal entities and their beneficial owners.

The characteristics, the establishment and operation of the Register, the procedure and securing the right or legitimacy of access to this, as well as any related issues referred to in the Law, are determined in the Directive, from the date the Register is kept, which are binding and mandatory with respect to their application to the persons to whom they are addressed – the Directive issued by the authority responsible for keeping the Register, specify the details and the method of application of the provisions of Article 61A of the Law applicable to the Company.

The information entered in the Register shall be adequate, accurate and up to date. The Company shall report to the Registrar of Companies and Official Receiver about any differences they identify between the information about the beneficial owner included in the Register and those at their disposal. It is understood that a corresponding reporting obligation is applicable to the authorities mentioned below (as per Article 61A(6)(a) of the Law), in the event that they identify such discrepancies and consider the report appropriate, provided that such reference does not unduly interfere with their respective functions. The Registrar of Companies and Official Receiver ensures that, via the Directive, the appropriate measures are taken for the timely settlement of disputes and the possibility to include a relevant mention in the Register until the difference is resolved.

In any case, the following persons have access to the information about the beneficial owner through the Register:

(i) The competent Supervisory Authority, the Unit, the Customs and Excise Department, the Tax Department and the Police, without any restrictions;
(ii) the Company, in the context of undertaking due diligence measures and customer identification procedures, as defined in the Law – it is provided that the Company is not permitted to solely depend on the information contained in the Register for the fulfillment of the requirements of due diligence measures and customer identification procedures, as specified in the Law, and based on a risk-based approach;
(iii) a member of the general public has access to the name, the month and year of birth, nationality and country of residence of the beneficial owner, as well as the type of and the extent of the rights he/she holds.

The Registrar of Companies and Official Receiver applies the access to information about the beneficial owner, as provided for in (ii) and (iii) above, under the condition of electronic registration and payment of a fee specified in Paragraph 10 of the Directive, which does not exceed the administrative costs of making the information available, including the costs of maintaining and developing the Register.

The competent Supervisory Authority, the Unit, the Customs and Excise Department, the Tax Department the Police have fast and unlimited access to all information held in the Register, without notifying the Company for that access. The Company has fast access to the Register when undertaking due diligence and customer identification measures, as defined in the Law. The persons referred to in (iii) above, have access to the Register, on the basis of the access rights provided for in Article 61A(7) of the Law.

The competent Supervisory Authority, the Police, the Customs and Excise Department, the Tax Department and the Unit provide timely and free-of-charge information, as referred to in Article 61A of the Law, to the corresponding competent authorities and Units of other Member States.

In exceptional cases, which are specified in Paragraph 15 of the Directive, may provide for case-by-case exceptions to access to all or part of the information about the beneficial owner where the access obtained by the persons referred to in (ii) and (iii) above, would expose the beneficial owner, to a disproportionate level, to risk of fraud, abduction, blackmail, extortion, harassment, violence or intimidation or if the beneficial owner is a minor or otherwise legally incompetent – the exemptions provided are not applicable to credit institutions or financial institutions.

Based on the Directives issued under the provisions of Article 61A of the Law, a person can apply to the Registrar of Companies and Official Receiver, for an exemption from disclosure of information relating to the beneficial owner. The decision of the Registrar of Companies and the Official Receiver in relation to a request for exemption from disclosure of data for the beneficial owner, is subject to appeal under the provisions of Article 146 of the Constitution. It is understood that no decision, decree or notification of the Registrar of Companies and Official Receiver in an exemption application, becomes executable before the expiration of seventy-five (75) days from the notification to the applicant, or while an action is pending against the said decision, pursuant to the provisions of Article 146 of the Constitution.

The Registrar of Companies and Official Receiver issues public annual statistics on the number of exemptions granted under the provisions of Article 61A(9)(a) of the Law, and their reasons on which these was based and submits the relevant data to the Commission.

The Registrar of Companies and Official Receiver keeps information on the beneficial owners of the Company, that is registered and has its registered office in the Republic. The Registrar of Companies and the Official Receiver may determine, as per Paragraph 5 of the Directive, the information communicated to the Register, as well as the procedure and time limits for their notification of companies and legal entities.

The Company, as well as every Company shall update the Register with the details of the final beneficial owners (natural persons), on the basis of Paragraph 5 of the Directive. This obligation for updating the Registry, exists with respect to a change in the beneficial owner of the Company within the time frame specified in the Directive.

A person who refuses, omits or neglects to fulfill reporting obligations for the beneficial owners of the Company, such as these obligations arise under the provisions of Article 61A of the Law and the Directive, is subject to a fine of two hundred euros (€200) and a further monetary fine of one hundred euros (€100) for each day of the continued infringement, with a maximum charge of twenty thousand euros (€20,000).

A person who, following a relevant warning from the authority responsible for keeping the Register:

(i) refuses, omits or neglects to fulfill reporting obligations for the beneficial owners of the Company, such as these obligations arise under the provisions of Article 61A of the Law and the Directive, and / or

(ii) when providing information to the Registrar of Companies and Official Receiver for the purpose of fulfilling reporting obligations for the beneficial owners of the Company, such as these obligations arise under the provisions of Article 61A of the Law and the Directive, proceeds, knowingly, with a statement that is false, misleading or deceptive for the beneficial owners of the Company,

is guilty of an offense and, if convicted, is subject to imprisonment not exceeding one (1) year or a fine penalty not exceeding one hundred thousand euros (€100,000) or both these sentences.

The Company and any of its members of the board of directors, the general manager, the secretary or another Company official or other governing body of the Company, who is proven to have consented or co-operated performing an offence, as mentioned above, is criminally liable.

The Register referred to in this Section is interconnected with the European Central Platform set up pursuant to the provisions of Article 22(1) of Directive 2017/1132 and according to the technical standards and procedures determined by the implementing acts adopted by the Commission, in accordance with Article 24 of Directive 2017/1132 and Article 31a of the EU Directive.

The information on the Company's beneficial owners, including the details of the rights held by the beneficial owners, available through the system of interconnection of registers, established under the provisions of Article 22 of Directive 2017/1132, and in accordance with the provisions of paragraphs 6 and 7 of Article 61A of the Law.

The Registrar of Companies and the Official Receiver may define mechanisms and procedures in relation to the interconnection of the Register and specify measures and procedures to ensure that the information corresponding to the beneficial owners of the Company that are available through the system of interconnection of registers, are up-to-date.

The information on the Company's beneficial owners, including the details of the rights held by the beneficial owners, are available through the Register and the system of interconnection of registers, for a time period of up to ten (10) years from the deletion of the Company from a relevant register kept by the Registrar of Companies and Official Receiver, based on the Companies Law or any other legislation. It is understood that, after the lapse of five (5) years from the deletion of the Company from the respective register, the record-keeping of the above-mentioned information in the Register and access to this information is permitted only in the context of conducting an administrative or criminal investigation, pursuant to the provisions of the Law, by the Supervisory Authorities, as well as the Unit, the Tax Department, the Customs and Excise Department and the Police.

11.5 Data Protection, Record-Retention and Statistical Data

1. The processing of personal data under the Law is subject to the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data, as amended, and Regulation (EU) 2016/679.

2. Personal data shall be processed by the Company on the basis of the Directive only for the purposes of the prevention of money laundering and terrorist financing and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data on the basis of the Directive for any other purposes, such as commercial purposes, shall be prohibited.

3. The Company shall provide new Clients with the information required pursuant to Article 13 of the GDPR Regulation as amended before establishing a business relationship or carrying out an occasional transaction. Also, the Company shall provide information to their new Clients before starting a business relationship or conducting an individual transaction for the processing of personal data under the Law for purposes of preventing money laundering and terrorist financing.

4. Pursuant to Article 23 of Regulation (EU) 2016/679 on the protection of personal data, the Law revokes the right of access of the data of the data subject to the personal data concerning him/her and the processing which they undergo in the following cases:

   (a) For the purposes of properly performing the duties of the Company, or
   (b) In order not to impede the conduct of official or legal investigations, analyzes or proceedings for the purposes of the Law and to ensure that the prevention, investigation and detection of money laundering and terrorist financing.

5. In order to prevent money laundering and terrorist financing, the processing of personal data is considered, based on the provisions of the Law, as a matter of public interest.

12 EMPLOYEES' OBLIGATIONS – EDUCATION & TRAINING

12.1 Employees' Obligations

(a) The Company's employees shall be personally liable for failure to report information or suspicion, regarding money laundering or terrorist financing;
(b) The employees must cooperate and report, without delay, according to point (e) of Section 5.2, anything that comes to their attention in relation to transactions for which there is a slight suspicion that are related to money laundering or terrorist financing;
(c) According to the Law, the Company's employees shall fulfil their legal obligation to report their suspicions regarding Money Laundering and Terrorist Financing, after their compliance with point (b) above;
(d) The Company's employees must comply with the relevant data protection requirements.

The Company provides training on an annual basis to all staff to make its employees aware with regards to:

(i) systems and procedures for the prevention of money laundering and terrorist financing;
(ii) updates of the Law and the Directives issued by the CySEC;

(iii) the European Union's Directives with regard to the prevention of the use of the financial system for the purpose of money laundering and terrorist financing;
(iv) their statutory obligations for combating money laundering and terrorism financing and respective sanctions for non-compliance;
(v) the relevant data protection requirements.

In this regard, the AMLCO prepares and implements, on an annual basis (or whenever deemed necessary), an education and training program for staff depending on the needs of the Company regarding the prevention of using the financial system for money laundering. The training program is taught by the AMLCO but also from other External Professional Speakers/Experts, as applicable and/or as it may be deemed necessary.

The AMLCO evaluates the adequacy of the seminars and the training provided to the staff and in conjunction with the Back Office Department maintains detailed data regarding the seminars/ programs carried out, such as:

- Contents of the training;
- The date, title and duration of the seminar and the names of the trainers;
- Names of employees participating in the seminar/training by branch/department and by position (management staff, officers, newcomers etc.);
- The persons who were unable to attend the training accompanied with the reason for non-attendance;
- Whether the lecture/seminar was organized internally or offered by an external agency or consultants.

12.2 Education & Training

The Company must make its staff aware of the provisions is has put in place to comply with its AML/CFT obligations. The Company shall take steps to ensure that staff understand:

- The business-wide risk assessment, and how it affects their daily work;
- The Company's AML/CFT policies and procedures, and how they have to be applied; and
- How to recognise suspicious or unusual transactions and activities, and how to proceed in such cases.

The Company shall ensure that AML/CFT training is:

- Relevant to the Company and its business;
- Tailored to staff and their specific roles;
- Updated regularly; and
- Effective.

12.2.1 *Employees' Education & Training Policy*

(a) The AMLCO shall ensure that its employees are fully aware of their legal obligations according to the Law and the Directive, by introducing a complete ongoing education and training program of their employees' education and training program in the recognition and handling of transactions and activities which may be related to Money Laundering or Terrorist Financing;
(b) The timing and content of the training provided to the employees of the various departments will be determined according to the needs of the Company. The Company shall have in place a documented Annual Training Programme which will need to be approved by the Board;
(c) The frequency of the training can vary depending on to the amendments of legal and/or regulatory requirements, employees' duties as well as any other changes in the financial system of the Republic of Cyprus;
(d) The training program aims at educating the Company's employees on the latest developments in the prevention of Money Laundering and Terrorist Financing, including the practical methods and trends used for this purpose;
(e) the training program aims also at educating the Company's employees on the relevant and latest requirements in relation to the protection of personal data;
(f) The training program will have a different structure for new employees, existing employees and for different departments of the Company according to the services that they provide. On-going training shall be given at regular intervals so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments;
(g) Appropriate levels of AML/CFT training are provided to the BoD and all staff involved in the conduct of the business (including staff at outsourced service providers) and Enhanced training

is provided to senior management and staff in key AML/CFT roles to endure their knowledge remains adequate and up-to-date;

(h) The Training content is reviewed and updated on a regular basis to ensure it remains current and the training material is approved by senior management.

The AMLCO shall be responsible to evaluate and assess the level of the employees understanding of any AML training provided as well as well as their overall prevention of Money Laundering level knowledge through interviews or via electronic or written assessments/tests/questionnaires as deemed more practical in each case taking into consideration the small number of Company's employees.

When setting up a staff training, the AMLCO shall consider:

- which staff require training;
- what is the content of the training provided; (e.g. legal framework, transactions monitoring, procedures for reporting suspicious transactions/activities, typologies/case studies of suspicious activities etc.);
- what form the training will take;
- how often training should take place;
- how staff will be kept up-to-date with emerging risk factors for the regulated entity.

Further to the above, training can take many forms and may include:

- face-to-face training seminars;
- completion of online training sessions;
- attendance at AML/CFT conferences and participation in dedicated AML/CFT forums;
- practice group meetings for discussion of AML/CFT issues and risk factors;
- guidance notes, newsletters and publications on current AML/CFT issues.

Training must be provided to staff prior to commencing work on behalf of the Company, and after that, at a minimum on an annual basis, ensuring the delivery of regular training and updates as required.

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

12.2.2 *AMLCO Annual Education & Training Programme*

The Senior Management of the Company shall be responsible for the AMLCO of the Company to attend external training. Based on his/her training, the AMLCO will then provide training to the employees of the Company further to Section 12.2.1 above.

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

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

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

13 REPORTING TO SENIOR MANAGEMENT - THE BOARD OF DIRECTORS & THE CYSEC

- ➢ The AMLCO will provide, at least on an annual basis, to the Company's senior management a written report which must be submitted at the latest two months following the year end to the Board of Directors and the latest within three months following the year end to CySEC. The written report will include areas such as the following:
- ➢ Measures taken to ensure compliance with the Law and AML Directive;

- Information concerning the reviews and inspections performed by the AMLCO and any significant weaknesses that were identified;
- The number of any internal suspicion reports submitted by the employees of the Company concerning suspicious transactions;
- The number of any reports that have been submitted to MOKAS;
- Information, details or observations regarding the communication with the employees on money laundering preventive issues;
- In a summary form the total deposits of clients, who exceed the set limit of €10,000, as and where applicable;
- Information concerning the policies, measures, practices, controls and procedures followed by the Company in relation to high risk clients, the country of origin of these clients, transactions, etc.;
- Information on the systems and procedures applied by the Company for the ongoing monitoring of clients' accounts and transactions;
- Information concerning the training seminars attended by the AMLCO and employees of the Company;
- Information on the proposed training program for the next year.

The AMLCO must submit the Compliance Annual report together with the minutes of the Board meeting during which the report was discussed to the Commission via CySEC's portal. The abovementioned Report should be drafted taking into consideration the points raised issued by CySEC as provide in, inter alias, Circulars C033, C186, C189, C191 and C315.

APPENDIX 1

AML Suspicious Activity Report Form

For Internal Use Only

Reporter Information

***Employee Full Name:** ***Employee Telephone + Ext.:**

***Employee Department:** ***Employee Position:**

Client Information (natural/legal – indicate as applicable)

***Full Name:** ***DOB:**
***Address:**
***Passport No.:** ***Expiration Date:**
***Company Registration No.:**
***Country of Residence/Information:**
***ID Card No.:** ***Nationality:**
***Tel/Fax/Email:** ***Other ID:**

Details of Suspicious Activity (Information/Transaction) – Please provide the reasons and a description of the nature of the suspicious activity identified; include details of persons you have dealt with and relevant dates – if possible, and/or any other relevant information that may assist us in investigating the activity.

****Details including any monetary amounts involved:***

****Describe why this activity is suspicious:***

****Other Investigation Comments:***

Date: **(DD/MM/YYYY)**

Reporter's Full Name **Reporter's Signature:**

*** All fields with * are mandatory and must be completed**
**** "Tipping off" the client in respect of any suspicions you, and the firm, may have is a criminal offence.**
*****Submit the form directly to the Compliance Officer.**

APPENDIX 2

AML Suspicious Activity CO Evaluation Form

For Internal Use Only

Anti-Money Laundering Compliance Officer Use (***to be filled by the Compliance Officer Only***)

***CO/AMLCO Full Name**:

***Date Received: (DD/MM/YYYY):**

***Time Received:**

**** Investigation Comments:***

***Reporting to MOKAS**

Yes ☐
No ☐
***If Yes: Please indicate: Date (DD/MM/YYYY) / GO-AML Ref. No.:**
***If No: Please justify reasons below:**

Other Comments:

***CO/AMLCO Name:**
***Position:**
***Internal Reference No.:**
***GO-AML Ref. No:**
***Date:**
***Signature:**

*** All fields with * are mandatory and must be completed**
**** "Tipping off" the client in respect of any suspicions you, and the firm, may have is a criminal offence.**

APPENDIX 3

EXAMPLES OF SUSPICIOUS TRANSACTIONS/ACTIVITIES RELATED TO MONEY LAUNDERING AND TERRORIST FINANCING

A. MONEY LAUNDERING

1. Transactions with no discernible purpose or are unnecessarily complex.

2. Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the Client.

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

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

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

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

7. There are frequent transactions in the same financial instrument without obvious reason and in conditions that appear unusual (churning).

8. There are frequent small purchases of a particular financial instrument by a Client who settles in cash, and then the total number of the financial instrument is sold in one transaction with settlement in cash or with the proceeds being transferred, with the Client's instructions, in an account other than his usual account.

9. Any transaction the nature, size or frequency appear to be unusual, e.g. cancellation of an order, particularly after the deposit of the consideration.

10. Transactions which are not in line with the conditions prevailing in the market, in relation, particularly, with the size of the order and the frequency.

11. The settlement of any transaction but mainly large transactions, in cash.

12. Settlement of the transaction by a third person which is different than the Client which gave the order.

13. Instructions of payment to a third person that does not seem to be related with the instructor.

14. Transfer of funds to and from countries or geographical areas which do not apply or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.

15. A Client is reluctant to provide complete information when establishes a Business Relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with financial organisations, names of its officers and directors, or information on its business location. The Client usually provides minimum or misleading information that is difficult or expensive for the financial organisation to verify.

16. A Client provides unusual or suspicious identification documents that cannot be readily verified.

17. A Client's home/business telephone is disconnected.

18. A Client that makes frequent or large transactions and has no record of past or present employment experience.

19. Difficulties or delays on the submission of the financial statements or other identification documents, of a Client/legal person.

20. A Client who has been introduced by a foreign financial organisation, or by a third person whose countries or geographical areas of origin do not apply or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.

21. Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g. student, unemployed, self-employed, etc).

22. The stated occupation of the Client is not commensurate with the level or size of the executed transactions.

23. Financial transactions from non-profit or charitable organisations for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.

24. Unexplained inconsistencies arising during the process of identifying and verifying the Client (e.g. previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address and date of birth etc).

25. Complex trust or nominee network.

26. Transactions or company structures established or working with an unneeded commercial way. e.g. companies with bearer shares or bearer financial instruments or use of a postal box.

27. Use of general nominee documents in a way that restricts the control exercised by the company's board of directors.

28. Changes in the lifestyle of employees of the financial organisation, e.g. luxurious way of life or avoiding being out of office due to holidays.

29. Changes the performance and the behaviour of the employees of the financial organisation.

30. Lending (including mortgages) secured against the value of assets in other jurisdictions, particularly countries where it is difficult to ascertain whether the customer has legitimate title to the collateral, or where the identities of parties guaranteeing the loan are hard to verify.

B. TERRORIST FINANCING

1. Sources and methods

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

i. collection of membership dues and/or subscriptions

ii. sale of books and other publications

iii. cultural and social events

iv. donations

v. community solicitations and fund raising appeals.

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

APPENDIX 4

THIRD-COUNTRY JURISDICTIONS WHICH HAVE STRATEGIC DEFICIENCIES IN THEIR NATIONAL AML/CFT REGIMES WHICH POSE SIGNIFICANT THREATS TO THE FINANCIAL SYSTEM OF THE EUROPEAN UNION

A. High-risk third countries which have provided a written high-level political commitment to address the identified deficiencies and have developed an action plan with FATF

1. Pursuant to Commission Delegated Regulation (EU) 2016/1675:
   - ☐ Afghanistan
   - ☐ Bosnia and Herzegovina
   - ☐ Guyana
   - ☐ Iraq
   - ☐ Lao PDR
   - ☐ Yemen
   - ☐ Vanuatu
   - ☐ Uganda
   - ☐ Syria

2. Pursuant to Commission Delegated Regulation (EU) 2018/105:
   - ☐ Ethiopia

3. Pursuant to Commission Delegated Regulation (EU) 2018/212:
   - ☐ Sri Lanka
   - ☐ Trinidad and Tobago
   - ☐ Tunisia

4. Pursuant to Commission Delegated Regulation (EU) 2018/212:
   - ☐ Pakistan

B. High-risk third countries which have provided a high-level political commitment to address the identified deficiencies, and have decided to seek technical assistance in the implementation of the FATF Action Plan, which are identified by FATF Public Statement

1. Pursuant to Commission Delegated Regulation (EU) 2016/1675:
   - ☐ Iran

C. High-risk third countries which present ongoing and substantial money-laundering and terrorist-financing risks, having repeatedly failed to address the identified deficiencies and which are identified by FATF Public Statement

1. Pursuant to Commission Delegated Regulation (EU) 2016/1675:
   - ☐ Democratic People's Republic of Korea (DPRK)

APPENDIX 5

AML Manual Acknowledgment Form

I (Full Name: _____), with DOB. (DD/MM/YYYY: _____), and ID Number (_____), hereby consent and confirm that I have read, understood the updated and approved, by the Board of Directors on the (DD/MM/YYYY: _____), Revised Internal Operations Manual ("IOM") and related Policies & Procedures of ISWM Asset Management Ltd and agree to fully comply with the provisions of such documentation as these were provided to and acknowledged by myself on the (DD/MM/YYYY: _____)

……
Employee Full Name

……
Signature

……..
Date