ANTI MONEY LAUNDERING (AML) AND TERRORIST FINANCING (TF) POLICY & MANUAL

RISK MANAGEMENT AND PROCEDURES MANUAL FOR THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

ACU SA

July 2021

Version 1

Person responsible for Policy Implementation: Irina Gusak, Rajender Shukla

Monitoring: Chief Compliance Officer

Internal Audit to be done annually - by Independent Audit Agency

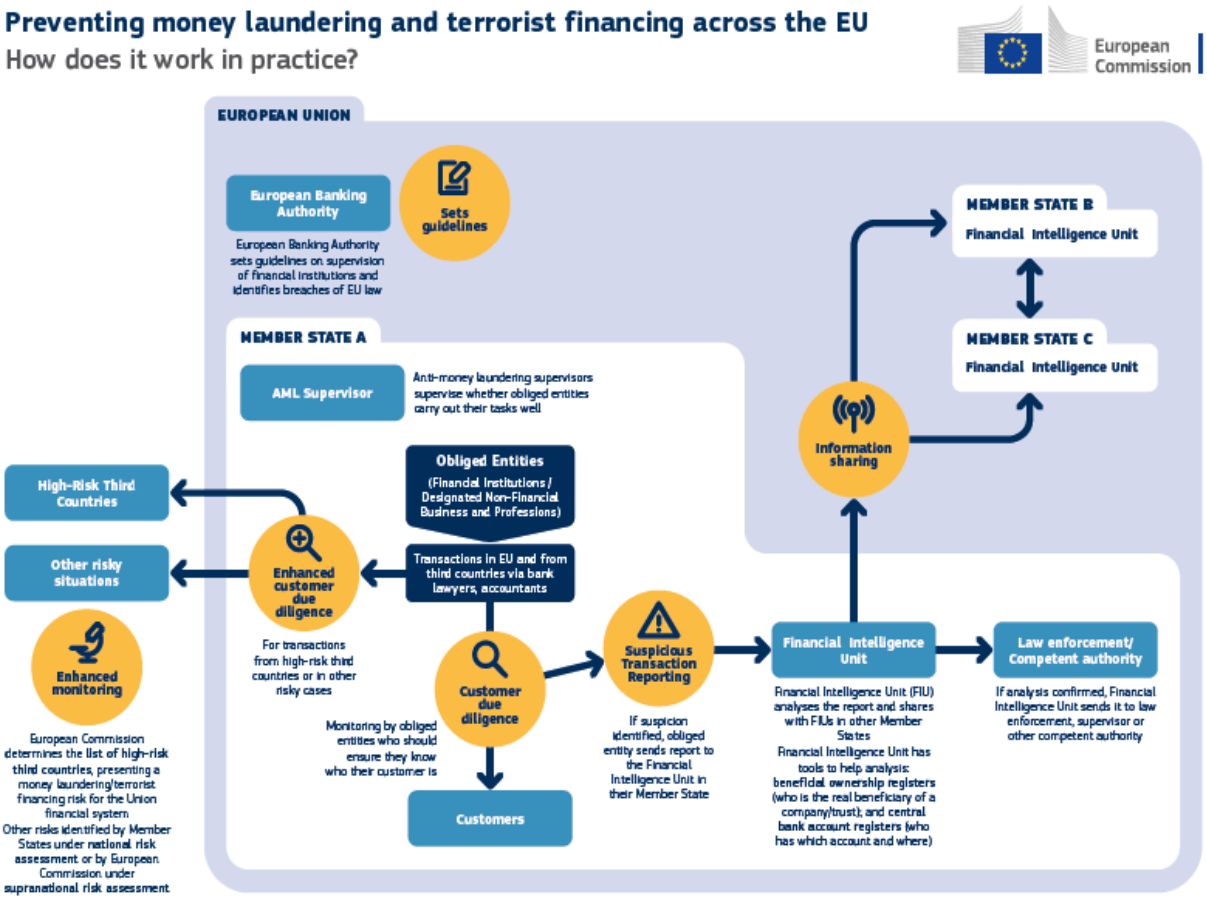


Table of Contents

1. **Introduction**

The Prevention- Anti Money Laundering Directives (Directive (EU) 2018/843 as amended (the " Directives") from time to time, recognizes the important role of the financial sector for the forestalling and effective prevention of money laundering and terrorist financing activities and places additional administrative requirements on all financial institutions, and business entities. the **European Commission** has adopted an action plan for a comprehensive Union policy on preventing money laundering and the financing of terrorism

The Risk Management and Procedures Manual for the Prevention of Money Laundering and Terrorist Financing (hereinafter the "**Manual**") is to equip the Company with the necessary internal practices, measures, procedures and controls that will assist the Company in the detection and prevention of Money Laundering and Terrorist Financing in accordance with the Directives regarding the prevention and suppression of money laundering and terrorist financing. The guidelines laid by the manual should be followed throughout the Company and all its personnel shall perform their duties as per the guidelines set out in this Manual and the relevant Company Operations Manuals.

1.1. Application

The Manual applies to all the services offered to the Company's Clients as well as all the relevant Company's dealings (Deposits, Withdrawal, Monitoring of the Clients Economic Profile and any Trading Patterns) with its Clients, irrespective of the Client's size of activities whereby there are any indications that the aforesaid Clients are involved in any of the Money Laundering and Terrorist Financing Activities.

In this respect, the Anti Money Laundering Compliance Officer (AMLCO) shall be responsible to update the Manual so as to comply with the Directives and future requirements, as applicable, regarding the Client identification and due diligence procedures.

1.2. Definition of Money Laundering

Money laundering is defined broadly and includes all forms of handling or possessing criminal property, including possessing the proceeds of one's own crime, and facilitating any handling or possession of criminal property. Criminal property may take any form, including money, securities, tangible property and intangible property. Money laundering can be committed in respect of the proceeds of offences that are considered as offences anywhere in the world irrespective of whether the offence was committed in another Country.

Businesses and individuals need to be alert of the risk of clients, their counterparties and others laundering money in any of its possible forms. The business or its client does not have to be a party to money laundering for a reporting obligation to arise.

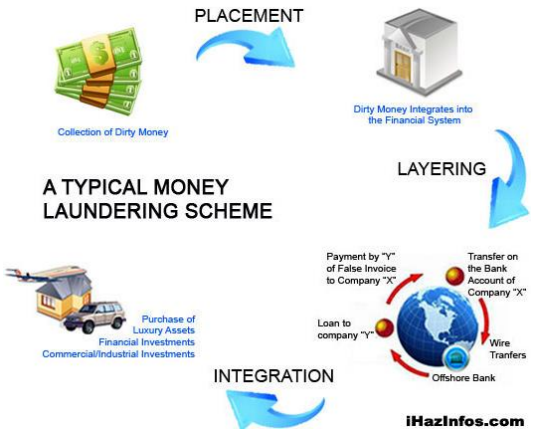
Money laundering is not only about cash transactions. Money laundering can be achieved through virtually every medium and financial institution or business.

For the purpose of this Manual, money laundering is also taken to encompass activities related to terrorist financing, including handling or possessing funds to be used for terrorist purposes/activities as well as proceeds from terrorism.

1.3. Stages for Money Laundering

There is no single method of laundering money. Despite the variety of methods employed, the laundering process is accomplished in three basic stages which may comprise transactions by the launderers that could alert a financial institution to criminal activity:

These three stages overlap and they should only be seen as a model rather than a rigid framework that is always followed.



A. Placement – Placement is the process where cash derived from criminal activity is infused into the financial system. When criminals are in physical possession of cash that can directly link them to criminal conduct. Such criminals need to place the cash into the financial system, usually through the use of bank accounts, in order to commence the laundering process.

This is the first stage in the washing cycle. Money Laundering (ML) is a "cash-intensive" business, generating vast amounts of cash from illegal activities (for example, street dealing of drugs where payment takes the form of cash in small denominations). The monies are placed into the financial system or retail economy or are smuggled out of the country. The aims of the launderers are to remove the cash from the location of acquisition so as to avoid detection from the authorities and then transform it into other asset forms; for example: travellers cheques, postal orders, etc.

Some placement methods are:

Disguised deposits: Launderers often divide large amounts of cash into a number of small transactions amounts, for example of less than €10,000 for instance:

- Making several deposits into a single or multiple account on successive days.
- Making deposits into a number of accounts (often opened by using false identities) at different branches of the same bank.
- Using different banks and then consolidating the accounts.
- Depositing cash into accounts of third parties such as lawyers, real estate agents, brokers and security firms.
- Depositing cash with the assistance of corrupt bank staff who themselves manipulate the deposits to make them appear as if they are below the reporting threshold.

Use of monetary instruments: Launderers purchase monetary instruments, such as money orders, postal orders and travellers cheques. In this way they convert cash into financial instruments for relatively small amounts, which are easily transportable, and then deposit them elsewhere.

Inter-mingling: Money launderers often attempt to conceal the origin of criminally derived cash by mixing it with legitimate generated cash. They do so by using the services of lawful business enterprises. A cheaper but riskier alternative is to establish what is known as a

"front company". This is a company that is incorporated on paper, but that does not own any physical assets and does not trade. The launderer opens an account in the name of the front company and deposits criminally derived cash into it, representing the money as the profits of the front company.

Assets purchases: Launderers may also use the cash proceeds of their criminal activities to buy assets like real estate, gold and precious metals, art, motor cars and antiques. These items may then be sold and converted back into cash.

Use of casinos: The extensive use of casinos both to place and integrate dirty money has emerged in recent years.

B. Layering – Layering usually involves a complex system of transactions designed to hide the source and ownership of the funds. Once cash has been successfully placed into the financial system, launderers can engage in an infinite number of complex transactions and transfers designed to disguise the audit trail and thus the source of the property and provide anonymity. One of the primary objectives of the layering stage is to confuse any criminal investigation and place as much distance as possible between the source of the ill-gotten gains and their present status and appearance.

Typically, layers are created by moving monies in and out of the offshore bank accounts of bearer share shell companies through Electronic funds' transfer (EFT). Given that there are over 500,000 wire transfers - representing in excess of $1 trillion - electronically circling the globe daily, most of which is legitimate, there isn't enough information disclosed on any single wire transfer to know how clean or dirty the money is, therefore providing an excellent way for launderers to move their dirty money. Other forms used by launderers are complex dealings with stock, commodity and futures brokers. Given the sheer volume of daily transactions, and the high degree of anonymity available, the chances of transactions being traced is insignificant.

A number of different types of transactions may be used at this stage of the laundering process, known as layering, aiming to disguise the proceeds of crime. The main methods of layering are:

Electronic (wire) transfers: Dirty money, once placed in the system, is often transferred by electronic fund transfer (wire transfers) between accounts or between banks, whether domestic

or offshore. Launderers might accumulate a number of small deposits in an account(s) and use a domestic electronic fund transfer to consolidate these accounts, followed by an international electronic fund transfer to move the monies offshore. This type of electronic money transfer can be carried out quickly and over vast distances, involving a number of offshore jurisdictions. Funds moved in this fashion, often in purported payment for goods sold or services rendered (that do not in reality exist), on a number of occasions, ultimately become practically untraceable.

Monetary instruments: Once placed in the banking system, dirty money can be used to buy cashier cheques, drafts, travellers cheques, letters of credit etc. These instruments may then be transported and transferred, either domestically or, more usually, offshore. Funds are first placed in the financial system onshore and are then moved offshore where the layering takes place. Once offshore the funds are often transferred between accounts held by front companies incorporated in offshore centres, where confidentiality provisions allow corporate service providers to act as nominees and/or for bearer shares to be issued in order to maintain anonymity in the outside world.

B. Integration – Integration is the stage at which laundered funds are reintroduced into the legitimate economy, appearing to have originated from a legitimate source. Integration is the final stage of the process, whereby criminally derived property that has been placed and layered is returned (integrated) to the legitimate economic and financial system and is assimilated with all other assets in the system. Integration of the "cleaned" money into the economy is accomplished by the launderer making it appear to have been legally earned. By this stage, it is exceedingly difficult to distinguish legal and illegal wealth.

Methods popular to money launderers at this stage of the game are:

Loan arrangements: The establishment of anonymous companies in countries where the right to secrecy is guaranteed. They are then able to grant themselves loans out of the laundered money in the course of a future legal transaction. Furthermore, to increase their profits, they will also claim tax relief on the loan repayments and charge themselves interest on the loan.

Sham transactions: sending of false export-import invoices overvaluing goods allows the launderer to move money from one company and country to another with the invoices serving to verify the origin of the monies placed with financial institutions.

Inheritance: Funds held in one jurisdiction on behalf of the launderer may be transferred to another jurisdiction and be purported to represent a gift or inheritance

Redemption of life policy or similar investment: This method involves the launderer in placing funds with an insurance company and sometime later encashing the property (or borrowing

against it) so that a cheque from the insurance company has the appearance of emanating from a legitimate source.

1.4. General Examples of Money Laundering Situations

Significant cash transactions: If a person is making thousands of dollars is small change a week from a business (something which is not unusual for a store owner) and wishes to deposit that money in a bank, it cannot be done without possibly drawing suspicion. In the United States, for example, cash transactions and deposits of more than a certain dollar amount are required to be reported as "significant cash transactions" to the Financial Crimes Enforcement Network (Fin CEN), along with any other suspicious financial activity which is identified as "suspicious activity reports". In other jurisdictions suspicion- based requirements are placed on financial services employees and firms to report suspicious activity to the authorities.

Irregular funding: One method of keeping this small change private would be for an individual to give money to an intermediary who is already legitimately taking in large amounts of cash. The intermediary would then deposit that money into an account, take a premium, and write a check to the individual. Thus, the individual draws no attention to himself, and can deposits his check into a bank account without drawing suspicion. This works well for one- off transactions, but if it occurs on a regular basis then the check deposits themselves will form a paper train and could raise suspicion.

Captive business: Another method involves establishing a business whose cash inflow cannot be monitored and passing the small change into this business and paying taxes on it. All bank employees however are trained to be constantly on the lookout for any transactions which appear to be an attempt to get around the currency reporting requirements. Such shell companies should deal directly with the public, perform some service- related activity as opposed to providing physical goods, and reasonably accept cash as a matter of business. Dealing directly with the public ensures plausible anonymity of source. An example of a legitimate business displaying plausible anonymity of source would be a hairstylist. Since it would be unreasonable for them to keep tract of the identity of their clients, a record of their transaction amounts must be accepted as a primary evidence of actual financial activity. Service- related business have the advantage of anonymity of resources. A business that sells computers has to account for where it actually got the computers, whereas a plumbing company merely has to account for labor, which can be falsified.

Corrupt politicians and lobbyists also launder money by setting up personal accounts to move money between trusted organizations, so that donations from inappropriate sources may be illegally used for personal gain.

Structuring ("smurfing"): Smurfing is possibly the most commonly used money laundering method. It involves many individuals who deposit cash into bank accounts or buy bank drafts in amounts under € 15,000 to avoid the reporting threshold.

Bank Complicity: Bank complicity occurs when a bank employee is involved in facilitating part of the money laundering process.

Money Services and Currency Exchanges: Money services and currency exchanges provide a service that enables individuals to exchange foreign currency that can then be transported out of the company. Money can also be wired to accounts in other countries. Other services offered by these businesses include the sale of money orders, cashiers' cheques, and traveler's cheques.
Asset Purchases with Bulk Cash: Money launderers may purchase high value item such as cars, boats or luxury items such as jewelry and electronics. Money launderers will use these items but will distance themselves by having them registered or purchased in an associate's name.
Electronic Funds Transfer: Also referred to as a telegraphic transfer or wire transfer, this money laundering method consists of sending funds electronically from one city or country to another to avoid the need to physically transport the currency.
Postal Money Orders: The purchase of money orders for cash allows money launderers to send these financial instruments out of the country for deposit into a foreign or offshore account.
Credit Cards: Overpaying credit cards and keeping a high credit balance gives money launderers access to these funds to purchases high value items or to convert the credit balance into cheques.
Casinos: Cash may be taken to a casino to purchase chips which can then be redeemed for a casino cheque.
Refining: This money laundering method involves the exchange of small denomination bills for larger ones and can be carried out by an individual who converts the bills at a number of different banks in order not to raise suspicion. This serves to decrease the bulk of large quantities of cash.
Legitimate Business/ Co- mingling of funds: Criminal groups or individual may take over or invest in business that customarily handles a high cash transaction volume in order to mix the illicit proceeds with those of the legitimate business. Criminals may also purchase business that commonly receive cash payments, including restaurants, bars, night clubs, hotels, currency exchange shops, and vending machine companies. They will then insert criminal funds as false revenue mixed with income that would not otherwise be sufficient to sustain a legitimate business.
Value Tempering: Money launderers may look for property owners who agree to sell their property, on paper, at a price below its actual value and then accept the difference of the purchase price "under the table". In this way, the launderer can, for example, purchase a €2 million, while secretly passing the balance to the seller. After holding the property for a period of time, the launderer then sells it for its value of €2 million.
Loan Back: Using this method, a criminal provides an associate with a sum of illegitimate money and the associate creates the paperwork for a loan or mortgage back to the criminal for the same amount, including all of the necessary documentation. This creates an illusion that the criminal's funds are legitimate.
The scheme's legitimacy is further reinforced through regularly scheduled loan payments made by the criminal and providing another means to transfer money.

1.5. Definition of Terrorism Financing

Terrorism is 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 definition of 'terrorist property' means that all dealings with funds or property which are likely to be used for the purposes of terrorism, even if the funds are 'clean' in origin, is a terrorist financing offence.

The main objective of Terrorism Financing (TF) is to build and maintain financial infrastructure to enable terrorists to fund and support their terrorist activities. Terrorist organisations need funds to plan their attacks and for terrorists' living and travel expenses. For example, the 9/11 attackers lived in the US for some time and had to not only fund their living expenses but also pay for direct costs associated with their planned attack, such as flying lessons. Terrorists also need substantial funds to finance their communication systems, training, propaganda and indoctrination programmes, for example to establish websites, television stations, training camps and indoctrination centres.

Although the sums needed to fund a terrorist attack are relatively small and can be hard to spot, the costs of establishing and maintaining a terrorist infrastructure are significant. You should be vigilant and look out for TF "red flags". ACU SA has listed the following TF indicators linked to financial transactions. Nonetheless, please note that the below list is not exhaustive and all employees should remain vigilant at all times:

- The use of funds by the non-profit is not consistent with the purpose for which it is established;
- The transaction was not economically justified considering the nature of the account holder's business or profession;
- A series of complicated transfer of funds from one person to another as a means to hide the source and intended use of funds;
- Transactions which are inconsistent with the account's normal activity;
- Deposits were structured below the reporting requirements to avoid detection;
- Multiple cash deposits and withdrawals with suspicious references;
- Frequent domestic and international ATM activity;
- No business rationale or economic justification for the transaction;
- Unusual cash activity in foreign bank accounts;
- Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country;
- Use of multiple, foreign bank accounts.

The following indicators may also be associated with TF cases:

- The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organisations;
- Use of false corporations, including shell-companies;
- Inclusion of the individual in the UN Sanctions list;

- Media reports that the account holder is linked to known terrorist organisations or is engaged in terrorist activities;
- UBO of account not properly identified;
- Use of nominees, trusts, family member or third-party accounts;
- Use of false identification;
- Abuse of non-profit organisation.

It is generally accepted that terrorism benefits from the following funding sources:

- State-sponsored terrorism (although UN sanctions have made this more difficult);
- Wealthy individuals sympathetic to their cause;
- Revenue generation (for example from crimes such as extortion, kidnapping, drug trafficking, counterfeit goods, or fraud; and
- Charitable contributions to non-profit organisations.

1.6. Money Laundering Offences

Every person who knows or ought to have known that any kind of property constitutes proceeds from criminal activities is guilty of an offence if he/she carries out any of the following:

i. Converts or transfers or removes such property for the purpose of concealing its illicit origin or of assisting any person who is involved in the commission of a offence to evade the legal consequences of his actions;

ii. Conceals or disguises the true nature, the source, location, disposition, movement, rights with respect to property or ownership of this property;

iii. Acquires, possesses or uses such property;

iv. Participates in, associates or conspires to commit or attempts to commit and aids and abets and provides counselling or advice for the commission of any of the above mentioned offences

v. Provides information with respect to investigations that are being performed for laundering offences for the purpose of enabling the person who acquired a benefit from the commission of a offence to retain the relevant proceeds or the control of the proceeds from the commission of the offence

Commitment of the above offences is punishable on conviction by a maximum of 14 years imprisonment or by a pecuniary penalty of up to Euro 500.000 or both of these penalties, in the case of a person knowing that the property proceeds are from an offence, or by a maximum of

5 years imprisonment or by a pecuniary penalty of up to Euro 50.000 or both of these penalties, in the case of ought to have known.

1.6.1. Other offences in connection with laundering and financing of terrorism offences (Failure to Report)

It is an offence for any person, including employees of the Company who, in the course of his trade, profession, business or employment, acquires knowledge or reasonable suspicion that another person is engaged in ML or TF not to report his knowledge or suspicion to Compliance officer, as soon as it is reasonably practical after the information came to his attention. Failure to report in these circumstances is punishable on conviction by a maximum of two (2) years' imprisonment or a fine not exceeding €5.000 or both of these penalties.

1.7. Predicate offences

Predicate offence is any offence that according to the Criminal Code is a Criminal Offence and this includes without limitation the following offences:

(a) drug trafficking;

(b) fraud;

(c) theft;

(d) premeditated and attempted murder;

(e) illicit importation, exportation, purchasing, selling disposition, possession, transfer and trafficking of arms and ammunitions;

(f) importation, exportation, purchasing, selling, disposition, possession, transfer of stolen objects, pieces of art, of antiquities and tokens of cultural heritage;

(g) detachment of money or of property of any kind by use or threat of use of force or other illicit act;

(h) living on the earnings of prostitution and offences associated with procuration and seduction of women and minors

(i) offences relating to corruption of public or private servants.

For the purposes of money laundering offences, it does not matter whether the predicate offence is subject to the jurisdiction of the any Courts or not.

The Law applies to the offences referred to as laundering offences and predicate offences. Conviction of any of the above offences is punishable by up to 14 years imprisonment and/or a fine up to €500.000 or both.

1.8. Responsibilities

This Manual will be subject to an ongoing review and update by the AML Compliance Department so as to ensure full compliance with current legislation & regulations.

This Manual and related policies, rules, operations and controls bind the members of the Board of Directors (hereafter refers as "BoD"), the Executives, Heads and Managers of the Company Divisions, the staff members, and any other person involved in the operations of the services offered. The primary responsibility lies with the Board of Directors which delegates operational responsibility to the Executives, Heads, and Managers of the Divisions.

The procedures and recommendation contained in this Manual must be followed strictly by the Company's personnel. Staff should be made aware of the seriousness of Money Laundering and Terrorist Financing activities, their own statutory obligations and be encouraged to co-operate and report suspicious transactions promptly. This can be done through the completion of the Internal Suspicion Report for Money Laundering and Terrorist Financing, which can be found in **APPENDIX I**, and should be submitted, to the Anti Money Laundering Compliance Officer **("AMLCO").**

It is the responsibility of all Company employees to read and understand the Company's Anti-Money Laundering and Terrorist Financing Manual. Each employee receives a copy of the Manual and has to sign that he/she has read and understood its contents and understands the responsibilities and procedures outlined in it.

All Company employees must follow any corrective measures the AMLCO may suggest during on-site visits or other forms of evaluation of procedures and controls to prevent money laundering and terrorist financing.

It is the duty and responsibility of the Head/Officer of the relevant Division to exercise the duties within his/her area of responsibility as itemized in this Manual, and be in line with the Policies of the Company, the Law, and any directives relevant to his/her area of responsibility.

The AMLCO ensures that the employees and divisions operate within the scope of the policies and rules outlined in this Manual.

2. Board of Directors

2.1 Board of Directors Duties:

The Board of Directors of the Company has the following duties:

(1) Determines, records and approves the general policy principles of the Company in relation to the prevention of money laundering and terrorist financing and communicates them to the compliance officer.

(2) Appoints a compliance officer and, where is necessary, assistant compliance officers and determines their duties and responsibilities, which are recorded in the risk management and procedures manual of paragraph 5.1

(3) Approves the Compliance Officer's Risk Management and Procedures Manual regarding Money Laundering and Terrorist Financing, which is communicated to all employees of the Company, that manage, monitor or control in any way the customers' transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined.

(4) Ensures that all requirements of the Law, especially the specified Procedures for preventing Money Laundering and Terrorist Financing of the Law and of the present Directive are applied, and assures that appropriate, effective and sufficient systems and controls are introduced for achieving the abovementioned requirement.

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

(6) Ensures that all employees are aware of the person who has been assigned the duties of the compliance officer, as well as his assistants, to whom they report any information concerning transactions and activities for which they have knowledge or suspicion that might be related to money laundering and terrorist financing. Such Information is provided to the Compliance Officer in a written report form (hereinafter to be referred to as "Internal Suspicion Report"), a specimen of such report is attached in the **APPENDIX I**.

(7) Establishes a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the compliance officer, either directly or through his assistants and notifies accordingly the compliance officer for its explicit prescription

in the risk management and procedures manual regarding money laundering and terrorist financing.

(8) Ensures that the compliance officer has sufficient resources, including competent staff and technological equipment, for the effective discharge of his duties.

(9) For assessing the Company's level of compliance with its obligations laid down in the Law and the present Directive the Directors assess and approves the Annual Report of the Compliance Officer and the Directors takes all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the aforesaid Annual Report.

(10) The Company will identify a member of the management board which will be responsible for the implementation of the law and of the applicable directives and/or circulars and/or regulations including any relevant acts of the European Union. The designated person responsible for the implementation of the legal framework related to the prevention and suppression of money laundering and terrorist financing shall have the necessary knowledge and expertise in order to meet the requirements of this role. The Board of Directors shall conduct a Board meeting to designate the responsible person and a formal approval by all members of the Board shall be taken. The designated responsible person will be assessed by the Board of Directors from time to time in order to ensure that the necessary implementations of the legal framework related to the prevention and suppression of money laundering and terrorist financing are in place

(11) To put in place appropriate procedures for its employees, or persons in a comparable position, to report breaches internally through a specific, independent and anonymous channel, proportionate to the nature and size of the Company.

2.2 Compliance Officer Appointment

The Directors appoint a compliance officer who belongs to the management of the Company so as to command the necessary authority.

Where it is deemed necessary due to the volume and/or the geographic spread of the services/activities, assistants of the compliance officer are appointed, by geographical district or otherwise for the purpose of assisting the compliance officer and passing internal suspicion reports to him.

The Company communicates immediately to the Commission, the names and positions of the persons it appoints as compliance officer and assistants of the compliance officer.

3. Obligations of the internal audit department

The internal audit department of the Company reviews and evaluates, at least on an annual basis, the appropriateness, effectiveness and adequacy of the policy, practices, measures, procedures and control mechanisms applied for the prevention of money laundering and terrorist financing. The findings and observations of the internal auditor are submitted, in a written report form, to the Board of Directors which decides the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected. The minutes of the abovementioned decision of the board of directors and the internal auditor's report are submitted to the Commission no later than four months after the end of the Calendar Year.

4. Executive Directors Duties

The Executive Directors of the Company approves the policies, procedures and controls applied by the obliged entity in relation to money laundering and terrorist financing, as well as monitor, and where appropriate, enhance the measures adopted. For the purposes of the above senior management means an officer or an employee of an obliged entity with sufficient knowledge of the obliged entities money laundering and terrorist financing risk exposure and with sufficient seniority to take decisions affecting its risk exposure. It is provided that the "senior management" may not be a member of the Board of Directors of the obliged entity

5. Anti-Money Laundering Compliance Officer (AMLCO)

The AMLCO shall belong hierarchically to the higher ranks of the Company's organizational structure (to the senior management) so as to command the necessary authority. Furthermore, the AMLCO shall lead the Company's Money Laundering Compliance procedures and processes and report to the Managing Director. The AMLCO shall also have access to all relevant information necessary to perform his duties. The level of remuneration of the AMLCO shall not compromise his objectivity.

5.1 Compliance Officer Duties (CO)

As a minimum, the compliance officer's duties include the following:

(a) to design, based on the general policy principles of the Company, the internal practice, measures, procedures and controls relevant to the prevention of Money Laundering and Terrorist Financing, and describe and explicitly allocate the appropriateness and the limits of responsibility of each department that is involved in the abovementioned. It is provided that, the above measures and procedures for the prevention of the abuse of new technologies and

systems providing financial services, for the purpose of Anti-Money Laundering and Terrorist Financing is appropriately considered and managed in the course of daily activities of the Company with regard to the development of new products and possible changes in the Company's economic profile (e.g. penetration into new markets)

(b) Develops and establishes the customers' acceptance policy and submits it to the board of directors for consideration and approval.

(c) Prepares a risk management and procedures manual regarding money laundering and terrorist financing.

(d) Monitors and assesses the correct and effective implementation of the policy principles of the Company in relation to the prevention of money laundering and terrorist financing, the practices, measures, procedures and controls and in general the implementation of the risk management and procedures manual for the same matters. In this regard, the Compliance Officer applies appropriate monitoring mechanisms (e.g. on-site visits to different departments of the Company) which will provide him/her all the necessary information for assessing the level of compliance of the departments and employees of the Company with the procedures and controls which are in force. In the event that he identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, gives appropriate guidance for corrective measures and where deems necessary informs the board of directors.

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

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

(g) If following the evaluation described in point (f), the compliance officer decides to notify BoD, then he completes an online report and submit it online to the Commission (hereinafter to be referred to as "Compliance Officer's Report to the Unit for Combating Money Laundering") the soonest possible (a template of which can be found in **APPENDIX II**).

It is provided that, after the submission of the compliance officer's report to the Commission, the accounts involved and any other connected accounts, are closely monitored by the compliance

officer and following any directions from commission, thoroughly investigates and examines all the transactions of the accounts.

(h) If following the evaluation described in point (f) the compliance officer decides not to notify the commission, then he fully explains the reasons for such a decision on the "Internal Evaluation Report" which is attached in the **APPENDIX III**.

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

(j) Ensures the preparation and maintenance of the lists of customers categorized following a risk based approach, which contains, inter alia, the names of customers, their account number, the date of the commencement of the business relationship and the date of termination (if applicable). Moreover, ensures the updating of the said lists with all new or existing customers, in the light of additional information obtained.

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

(l) Evaluates the systems and procedures applied by a third person on whom the Company relies for customer identification and due diligence purposes, according to section 7.12 of this manual, and approves the cooperation with it.

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

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

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

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

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

(r) Prepares the annual report that assesses the Company's level of compliance with its obligations laid down in the Law and the present Directive.

(s) Responds to all requests and queries from Commission, provides all requested information and fully cooperates with the Commission.

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

(u) To maintain, update and communicate accurate and up-to-date information in relation to the beneficial owner of an express trust or similar legal arrangement, in case where the Company acts as trustee or as a legal person holding equivalent position in similar legal arrangement.

During the execution of his duties and the control of the compliance of the Company with the Law and the present Directive, the compliance officer obtains and utilizes data, information and reports issued by international organizations referred later in this manual.

5.2 Appointment of Alternate AML Compliance Officer

The Company shall appoint temporarily an Alternate AML Compliance Officer, when the AML Compliance Officer is absent. It is clarified that the provisions of paragraph 8 of the Directive do not apply when the AML Compliance Officer resigns from his/her position, since in such case the Company should appoint a new AML Compliance Officer.

The Alternate Compliance officer shall perform all the duties of the AML Compliance Officer as indicated in this Manual when is absent. The Company shall make sure that the Alternate Compliance officer shall fulfil the requirements in regards to the appointment of an AML Compliance Officer. The Company may appoint an external Alternate Compliance officer provided that the appointment concerns a physical person.

5.3 Compliance Officer's Annual Report

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

(2) The Annual Report is prepared and submitted for approval to the Board of Directors, within two months from the end of each calendar year (the latest by the end of February).

(3) The Annual Report, after its approval by the Board of Directors, is submitted to whom it may concern together with the minutes of the meeting, during which the Annual Report has been discussed and approved. It is provided that the said minutes include the measures decided for the correction of any weaknesses and/or deficiencies identified in the Annual Report and the implementation timeframe of these measures.

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

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

(b) Information on the inspections and reviews performed by the compliance officer, reporting the material deficiencies and weaknesses identified in the policy, practices, measures, procedures and controls that the Company applies for the prevention of money laundering and terrorist financing. In this regard, the report outlines the seriousness of the deficiencies and weaknesses, the risk implications and the actions taken and/or recommendations made for rectifying the situation.

(c) The number of internal suspicion reports submitted by employees of the Company to the compliance officer and possible comments/observations thereon.

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

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

(f) Information on the policy, measures, practices, procedures and controls applied by the Company in relation to high risk customers as well as the number and country of origin of

high risk customers with whom a business relationship is established or an occasional transaction has been executed.

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

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

(i) Information on the training courses/seminars attended by the compliance officer and any other educational material received.

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

(k) 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 compliance officer as well as recommendations and timeframe for their implementation, for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against money laundering and terrorist financing.

5.4 Monthly prevention statement

The AMLCO shall prepare "Monthly prevention statement regarding the prevention of Money Laundering and Terrorist Financing", which includes details as regards the total cash deposits accepted by the Company, the Internal Suspicions Reports, and the AMLCO's Reports to the Unit, according to points (e) and (g) in Section 8.2 of the Manual, respectively.

6. Application of Appropriate Measures and Procedures on a Risk Based Approach

6.1. Application of measures and procedures on a risk based approach

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

A risk-based approach:

(a) recognizes that the money laundering or terrorist financing threat varies across customers, countries, services and financial instruments;

(b) allows the Board of Directors to differentiate between customers of the Company in a way that matches the risk of their particular business;

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

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

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

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

(a) identifying and assessing the money laundering and terrorist financing risks emanating from particular customers, financial instruments, services, countries and geographical areas of operation, services and transactions or delivery channels for providing banking of the Company and its customers;

(b) documenting in the risk management and procedures manual, the policies, measures, procedures and controls to ensure their uniform application across the Company by persons specifically appointed for that purpose by the board of directors;

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

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

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.

6.2. Identification, recording and evaluation of risks

(1) The compliance officer has the responsibility to detect, record and evaluate at least on an annual basis all potential risks that the Company is facing. The successful establishment of measures and procedures on a risk-based approach requires the clear communication of the measures and procedures that have been decided across the Company, along with robust mechanisms to ensure that these are implemented effectively, weaknesses are promptly identified, and improvements are made wherever necessary.

(2) A risk-based approach involves the identification, recording and evaluation of the risks that have to be managed. The Company assesses and evaluates the risk it faces, for usage of the services provided for the purpose of money laundering or terrorist financing. The particular circumstances of the Company determine the suitable procedures and measures that need to be applied to counter and manage risk.

(3) In the cases where the services that the Company provides are relatively simple, involving relatively few customers, or customers with similar characteristics, then the Company applies procedures that focus on those customers who fall outside the 'norm'.

(4) The identification, recording and evaluation of risk that the Company faces presupposes the finding of answers to the following questions:

(a) What risk is posed by the Company's customers? For example:

i. complexity of ownership structure of legal persons,

ii. companies with bearer shares,

iii. companies incorporated in offshore centres,

iv. politically exposed persons,

v. customers engaged in transactions which involves significant amounts of cash,

vi. customers from high-risk countries or from countries known for high level of corruption or organized crime or drug trafficking;

(b) What risk is posed by a customer's behaviour? For example:

i. customer transactions where there is no apparent legal financial/commercial rationale,

ii. situations where the origin of wealth and/or source of funds cannot be easily verified,

iii. unwillingness of customers to provide information on the beneficial owners of a legal person;

(c) How did the customer communicate the Company? For example:

i. non face to face customer,

ii. customer introduced by a third person;

(d) What risk is posed by the services provided to the customer? For example:

i. services that allow payments to third persons,

ii. large cash deposits or withdrawals.

(5) The application of appropriate measures and the nature and extent of the procedures of a risk based approach depends on different parameters. Indicative parameters are the following:

(a) the scale and complexity of the services;

(b) geographical spread of the services and customers;

(c) the nature (e.g. non face to face customer) and economic profile of customers as well as of financial instruments and services offered;

(d) the distribution channels and practices of providing services;

(e) the volume and size of transactions;

(f) the degree of risk associated with each area of services;

(g) the country of origin and destination of customers' funds;

(h) deviations from the anticipated level of transactions;

(i) the nature of business transactions.

6.3. Design and implementation of measures to manage and mitigate the risks

The most commonly used risk categories and the categories that the Company takes into account as a minimum, are the following:

- Country/Geographical risk
- Service risk
- Client risk
- Delivery channels risk

In practice, these risks may overlap and should be viewed as inter-related. There is no single methodology to apply to these risk categories, and their application is merely intended to provide a suggested framework for approaching the management of potential risks. When implementing RBA, the assessment of risks may change according to time and global developments. A static implementation of the RBA may lead to a distorted picture and complicated circumstances, increasing the business risks of each firm.

(1) When the Company through its Compliance Officer identifies, record and evaluates the risks it faces, then designs and implements the appropriate measures and procedures for the correct management and mitigation, which involve without limitation: the verification of the customers identity, the collection of information for the construction of their economic profile and monitoring their transactions and activities.

(2) Taking into consideration the assessed risk, a Company determines the type and extent of measures it adopts, to manage and mitigate the identified risks cost effectively. These measures and procedures may, for example, include:

(a) adaptation of the customer due diligence procedures in respect of customers in line with their assessed money laundering and terrorist financing risk;

(b) requiring the quality and extent of requisite identification data for each type of customer to be of a certain standard (e.g. documents from independent and reliable sources, third person information, documentary evidence);

(c) obtaining additional data and information from the customers, where this is appropriate for the proper and complete understanding of their activities and source of wealth and for the effective management of any increased risk emanating from the particular business relationship or the occasional transaction; and

(d) on going monitoring of high risk customers' transactions and activities.

(3) The risk assessment and the implementation of the measures and procedures of paragraph (2) result in the categorisation of customers according to the Customer Acceptance Policy. The said 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. In addition, the Company when assessing the risk of money laundering and terrorist financing should take into account, among others, the Risk Factor Guidelines and any guidelines/guidance issued by the Financial Action Task Force (FATF).

(4) The category of low risk customers is further defined in the Customer Acceptance Policy.

(5) The category of high risk customers, is also further defined in the Customer Acceptance Policy and includes the Non Face to Face customers as well as any other customer determined by the Law and the Directive, the Company itself and by its Customer Acceptance Policy to be classified as such.

(6) The Company prepares and maintains list for all the categories of customers, which contain, inter alia, the customers' names, account numbers, and date of commencement of business relationship. The said lists should be promptly updated with all new or existing customers that the Company has determined, in the light of additional information received by taking into consideration factors such as the customer's background, type and nature of its business activities, its country of origin, the services and the financial instruments applied for, the anticipated level and nature of business transactions as well as the expected source and origin of funds.

(7) The Company is, at all times, in a position to demonstrate to the Commission that the extent of measures and control procedures that applies are proportionate to the risk it faces for the use of services provided, for the purpose of money laundering or terrorist financing.

(8) In view of this, documenting the measures and procedures set out in paragraphs 2-6 above will assist the Company to prove:

(a) the ways used to identify, record and assess the risk of its services being used for money laundering or terrorist financing;

(b) how it has determined the introduction and implementation of specific measures and procedures for the management and mitigation of risks; and

(c) the methods applied for monitoring and improving, whenever deemed necessary, the specific measures, procedures and controls.

6.4. Monitoring and improving the measures and procedures

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

6.5. Dynamic risk management

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Customers' activities change as well as the services and financial instruments provided by the Company change.

6.6. Relevant international organizations

On implementing appropriate measures and procedures on a risk based approach, and on implementing the customer identification and due diligence procedures the compliance officer, consults data, information and reports [e.g. customers from countries which inadequately apply Financial Action Task Force's (FATF), country assessment reports that are published in following relevant international organizations:

(a) FATF - www.fatf-gafi.org·

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

(c) the EU Common Foreign & Security Policy (CFSP)- http://ec.europa.eu/external_relations/cfsp/sanctions/lis t/consol-list.htm·

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

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

(f) the International Monetary Fund (IMF) – www.imf.org.

(g) European Commission website - https://ec.europa.eu/commission/index_en

(h) The Joint Committee European Supervisory Authorities - https://esasjoint-committee.europa.eu/;

(i) The EU Sanctions Map - https://www.sanctionsmap.eu/#/main;

(j) The Ministry of Foreign Affairs of Germany - http://www.mfa.gov.cy/mfa/mfa2016.nsf/mfa35_en/mfa35_en?OpenDocument

(k) OFAC'S Specially Designated Nationals List (SDN List) - https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx

(l) COMMISSION DELEGATED REGULATION (EU) 2020/855 of 7 May 2020 related to the high risk third countries - https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing/eu-policy-high-risk-third-countries_en

6.7. Sources of information to identify possible ML/TF risk

(1) Where possible, information about these ML/TF risk factors should come from a variety of sources, whether these are accessed individually or through commercially available tools or databases that pool information from several sources. The Company should determine the type and numbers of sources on a risk-sensitive basis.

(2) The Company should always consider the following sources of information:
• the European Commission's supranational risk assessment;
• information from government, such as the government's national risk assessments, policy statements and alerts, and explanatory memorandums to relevant legislation;
• information from regulators, such as guidance and the reasoning set out in regulatory fines;
• information from Financial Intelligence Units (FIUs) and law enforcement agencies, such as threat reports, alerts and typologies; and
• information obtained as part of the initial CDD process

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

6.8. Serious Tax Offences

A person who is proved that fraudulently omits or delays to pay the amount of tax which is required to pay under the law, is guilty of a criminal offence, punishable if convicted with imprisonment.
Additionally, according to Prevention and Suppression of Money Laundering and Terrorist Financing directives, the predicate offences are, amongst other, all criminal offences punishable

with imprisonment exceeding one year, as a result of which proceeds have been derived which may constitute the subject of a money laundering offence.
Based on the foregoing, fraudulent tax evasion is considered as “predicate offence”.
The Company should apply the following procedures and controls in order to determine whether there are reasonable grounds to suspect that client accounts contain proceeds derived from serious tax offences and when such is the case, it should proceed with the appropriate reporting obligations.
However, the Company is not expected to determine if its clients are fully compliant with all their tax obligations globally.
The Company following a risk based approach:

- Should implement adequate and appropriate systems and processes to detect, prevent and deter money laundering arising from serious tax offences;
- Should not knowingly aid or abet clients of prospects in committing tax offences;
- The Company:
- Should, when applying client due diligence measures, to screen clients against databases or third party checks for adverse tax-related news;
- Should conduct on-going monitoring of the business relationship with its clients and to ensure that the actual amount of funds deposited by clients are consistent with the amount of funds indicated at account opening, as well as with the economic profile of the client.
- In case of any suspicious of Tax Evasion a suspicious report will be prepared and submitted to the Money laundering Officer as described in relevant procedure in this manual “Internal reporting procedures and reported to the ‘’commission”.
- The Back Office department in cooperation with the Money laundering Officer are responsible for the implementation of above procedure and control.

7. Customer Identification and Due Diligence Procedures

7.1. Obligation for customer identification and due diligence procedures

The Company applies customer identification procedures and customer due diligence measures in the following circumstances:

(1) When establishing a business relationship;

(2) When carrying out an occasional transaction ;

(3) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold by virtue of the Law;

(4) When there are doubts about the veracity or adequacy of documents, evidence, or information that were obtained previously for the verification of identity of an existing customer.

7.2. Time of Application of Due Diligence Measures and Identification Procedures

(1) The Company verifies the identity of the client and the beneficial owner (KYC) know your customer, before the establishment of a business relationship or the carrying out of an occasional transaction.

(2) By way of derogation from paragraph (1), the identification the verification of the identity of the customer and the beneficial owner may be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring. In such situations these procedures shall be completed as soon as practicable after the initial contact and before any transactions take place.

7.3. Constant Monitoring and Updating of Customer Identification Records

(1) In addition to the provisions of the Law that refer to the obligation for customer identification and due diligence procedures, the Company ensure that the customer identification records remain completely updated with all relevant identification data and information throughout the business relationship. The Company examines and checks, on a regular basis, the validity and adequacy of the customer identification data and information it maintains, especially those concerning high risk customers. The procedures and controls of also determine the timeframe during which the regular review, examination and update of the customer identification is conducted. The outcome of the said review is recorded in a separate note/form which should be kept in the respective customer file.

(2) Despite the provisions of paragraph (1) and taking into consideration the level of risk, if at any time during the business relationship, the Company becomes aware that reliable or adequate data and information are missing from the identity and the economic profile of the customer, then takes all necessary action, by applying the customer identification and due diligence procedures according to the Law and the present Directive, to collect the missing data and information, the soonest possible, so as to identify the customer and update and complete the customer's economic profile.

(3) In addition to the provisions of paragraphs (1) and (2), the Company checks the adequacy of the data and information of the customer's identity and economic profile, whenever one of the following events or incidents occurs:

(a) A transaction takes place which appears to be unusual and/or significant compared to the normal pattern of transactions and the economic profile of the customer, with the expected turnover as declared at the establishment of the business relationship.

(b) significant deviations are investigated by the relevant department and the findings are kept in the respective client's file. In case no additional information provided by the client if a significant deviation is detected, then the Company may terminate the business relationship with the said client.

(c) a material change in the customer'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 undertake new major business activities;

(d) a material change in the way and the rules the customer operates.

(4) Transactions that cannot be justified with the available information taken by the Company, shall be assessed and reviewed, so as to determine whether suspicious transactions in relation to money laundering or terrorist financing exist. In this case the relevant person identified the suspicious transaction shall submit an internal suspicious report to the Compliance officer and afterwards the relevant procedure shall be followed as per 9.1 Section of this manual.

(5) Checks on a constant basis the validity and adequacy of customer's information (KYC + economic profile). Specifically, the Company set the following timeframe for the said checks based on the client categorisation:

- For High Risk Clients every one (1) year
- For Normal Risk Clients every (2) years
- For Low Risk Clients every three (3) years.

7.4. Customer Identification and Verification Procedures by Type

7.4.1. Customer Identification, Verification and Due Diligence Measures shall comprise:

(1) The Company in dealing with any person (whether physical or legal) is satisfied that it's dealing with a real person and, for this reason, obtains sufficient evidence of identity to verify that the person is who he claims to be.

(2) Furthermore, the Company verifies the identity of the beneficial owners of the customers' accounts. In the cases of legal persons, the Company obtains adequate data and information so as to understand the ownership and control structure of the customer.

(3) Additionally the Company verifies the identity of the Directors, Signatories and Shareholders for all types of Customers.

(4) 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.

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

(6) A person's residential and business address is an essential part of his identity and, thus, a separate procedure for its verification is achieved through the following manner:

the production of a recent (up to 6 months) utility bill, local authority tax bill or a bank statement or any other document same with the aforesaid (to protect against forged or counterfeit documents, the prospective customers are required to produce original documents).

(7) It is never acceptable to use the same verification data or information for verifying the customer's identity and verifying its home address.

(8) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;

(9) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

(10) The Company shall apply the Customer Identification and Due Diligence measures mentioned above and in this Section but in applying the aforesaid measures the Company may determine the extent of such measures on a risk-sensitive basis when assessing the risks of money laundering and terrorist financing by taking into account at least the variables set out in **APPENDIX IV** of this manual

Translation of Customer Identity Verification Documents and Other Documents

(1) The Company for Compliance with the Law and the Directive provides a true translation of any documents/data that has obtained and that are in languages other than German or English and the Company translates them either internally by an employee of the Company who is fluent in English and in the language of the translated document or alternatively translates such Documents/Data externally through a professional translator. Exact and Full translation is required by the person that will translating the documents/data including any stamps and any other phrases or indicators not included in the main body of the document.

(2) Such translator shall put the date and his signature on the translated document. Sample of the True Translation Form is provided in **APPENDIX XI**. The initial document and its True Translation in the aforesaid type and manner shall be kept together in electronic form and in hard copy in the relevant client's file.

7.4.2. Identification Procedures for all Type of Customers

7.4.2.1. Natural persons residing in the Country

(1) The Company ascertain the true identity of natural persons who are residents of the Country by obtaining the following information:

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

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

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

iv.e-mail address , if any,

v.date and place of birth,

vi.nationality and

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

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

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

i. visit at the place of residence (in such a case, the Company's officer who carries out the visit prepares a memo which is retained in the customer's file), and
ii. the production of a recent (up to 3 months) utility bill, local authority tax bill or a bank statement or any other document same with the aforesaid (to protect against forged or counterfeit documents, the prospective customers are required to produce original documents).

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

7.4.2.2. Natural persons not residing in the Country

(1) For customers who are not normally residing in the Republic the Company ascertain their true identity obtaining the following information:

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

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

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

IV. e-mail address, if any,

V. date and place of birth,

VI. nationality and

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

(2) In addition to the information collected according to paragraph (1), the Company, without prejudice to the application on a risk-sensitive basis, requires and receives information on public positions which the prospective customer holds or held in the last twelve months as well as whether he is a close relative or associate of such individual, in order to verify if the customer is a politically exposed person, according to section 7.11.3.

(3) For those customers not residing in the country, passports are always requested and, if available, official national identity cards issued by competent authorities of their country of origin are obtained and certified true copies of the pages containing the relevant information from the said documents are obtained and kept in the customers' files.

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

(5) Other Practical Measures for the verification of the Clients Identity can be found on Section 0.

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

7.4.2.3. Legal Entities

(1) According to the Law for customers that are legal entities, it is established that the natural person appearing to act on their behalf, is appropriately authorised to do so and his identity is established and verified according to the procedures set in this section of the manual.

(2) The Company takes all necessary measures for the full ascertainment of the legal entities 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 entity.

(3) The verification of the identification of a legal entity that requests the establishment of a business relationship or the execution of an occasional transaction, comprises the ascertainment of the following:

i. the registered number,

ii. the registered corporate name and trading name used,

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

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

v. the members of the Board of Directors,

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

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

viii. The economic profile of the legal entity,

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

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

ii. certificate of registered office,

iii. certificate of Directors and Secretary,

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

ix. Memorandum and Articles of Association of the legal entity,

x. a resolution of the Board of Directors of the legal entity for entering into business Transaction with the company,

xi. 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,

xii. documents and data for the verification, according to the provisions of the present Directive, the identity of the persons that are authorised by the legal entity to execute documents, as well as the registered shareholders and beneficial owners of the legal entity.

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

(6) For legal entity incorporated outside the country, the Company requests and obtains documents similar to the above.

(7) As an additional due diligence measure, on a risk-sensitive basis, the Company may carry out a search and obtain information from the records of the Registrar of Companies and Official Receiver of the country (for domestic companies) or from a corresponding authority in the company's (legal entity) country of incorporation (for foreign companies) and/or request information from other sources in order to establish that the applicant company (legal entity) 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 country or by an appropriate authority outside the country.

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 entity, or any suspicions arise emanating from changes in the nature of the transactions performed by the legal entity, 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 entity and all additional documentation and information for updating the economic profile of the legal entity is collected.

(8) In the case of a customer-legal entity 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 entity, registered in the country or abroad, the Company, before establishes a business relationship or executes an occasional transaction, verifies the ownership structure and the identity of the natural persons who are the beneficial owners and/or control the other legal entity.

(9) Apart from verifying the identity of the beneficial owners, the Law requires that the persons who have the ultimate control over the legal entity's business and assets are identified. In the

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

(10) In cases where the beneficial owner of a legal entity, requesting the establishment of a business relationship or the execution of an occasional transaction, is a trust set up in the ountry or abroad, the Company implements the procedure provided in paragraphs **Error! Reference s ource not found.** and **Error! Reference source not found.** of this manual.

(11) The Company should obtain and hold adequate, accurate and current information on its beneficial ownership. The said information should be held, also, in the central register of corporate and any other legal entities established in the country ('Entities Registry').
The details regarding the establishment and operation of the Entities Registry will be determined in Regulations.
The access to the beneficial ownership information, both when held by corporate and other legal entities and when held in the Entities Registry, will be permitted to Supervisory Authorities and persons based on restrictions.

(12) Trustee or commissioner of any express trust obtains and holds adequate, accurate and up-to-date information on beneficial ownership regarding the trust.
The said information should be held in the central registry of trusts, as well, which will be established in the country ('Trusts Registry'), when the express trust generates tax consequences in the country.
The details regarding the establishment and operation of the Trusts Registry will be determined in Regulations.
The access to the beneficial ownership information, both when held by the trustee or commissioner and when held in the Trusts Registry, is based on restrictions.
The measures of the present sub-paragraph, also, to other types of legal arrangements with a structure or functions similar to trusts.

7.4.2.4. Nominees or agents of third persons

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

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

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

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

7.4.2.5. Politically exposed persons'

(1) The establishment of a business relationship with politically exposed persons as defined in paragraph 7.4.2.5(3), may expose a Company to enhanced risks, especially, if the potential customer seeking to establish a business relationship who is a politically exposed person.

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

(2) In order to effectively manage such risks, the Company assess the countries of origin of their customers in order to identify the ones that are more vulnerable to corruption or maintain laws and regulations that do not meet the requirements of the Financial Action Task Force.

With regard to the issue of corruption one useful source of information is the Transparency International Corruption Perceptions Index which can be found on the website of Transparency International at www.transparency.org. With regard to the issue of adequacy of application of the 40+9 recommendations of the FATF, the Company may retrieve information from the country assessment reports prepared by the FATF or other regional bodies operating in accordance with FATF's principles (e.g. Moneyval Committee of the Council of Europe) or the International Monetary Fund.

(3) "Politically Exposed Persons" or "PEPs" means natural persons who are or have been entrusted with prominent public functions' in the country or a foreign country or their immediate family members and persons known to be their close associates.

(a) Prominent Public Function shall mean any of the following public functions:

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

ii. members of parliaments or of similar legislative bodies

iii. members of the governing bodies of political parties;

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

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

vi. Ambassadors, and high-ranking officers in the armed forces,

vii. members of the administrative, management or supervisory bodies of State-owned enterprises.

viii. Directors, Deputy Directors and members of the board or equivalent function of an international organization.

ix. Mayors

None of the categories set out in section 7.4.2.5(3)of this section shall be understood as covering middle ranking or more junior officials.

(b) 'Immediate family members' includes the following:

i. the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person

ii. the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person

iii. the parents of a politically exposed person

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

i. any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in section 7.4.2.5(3).

ii. any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

(4) Without prejudice to the application, on a risk-sensitive basis, of the enhanced customer due diligence measures of section 7.10, where a politically exposed person is no longer entrusted

with a prominent public function by a Member State or a third country, or with a prominent public function by an international organisation within the meaning of section 7.4.2.5(3) of this Section, the Company shall, for at least 12 months, be required to take into account the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to politically exposed person .

7.4.2.6. Customers from countries which inadequately apply Financial Action Task Force's recommendations or included in the EU Commission's List of High Risk Third Countries

The Company may establish a business relationship with Customers from countries which inadequately apply Financial Action Task Force's recommendations or included in the EU Commission's List of High Risk Third Countries provided that the Company will apply the Identity Verification Procedures of Section 7.4 and the Enhanced Due Dilligence Measures of Section 7.10.

7.5. FATCA & CRS Reportable Information: General Requirements

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

The Company is obliged to review persons that are tax resident elsewhere and report this to the Commission if needed.

Company to update its questionnaire in line with compliances with the CRS/FATCA reporting obligations.

The Company through its questionnaire in addition to the Information required by paragraph 7.4, requires from its clients the following additional information:

(a) Taxpayer Identification Number(s) (TIN)

(b) Jurisdiction(s) of residence

(c) The account number (or a functional equivalent in the absence of an account number)

(d) The name and identifying number of the reporting financial institution

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

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

The Company is required to carry out due diligence procedures, in order to establish if the person is tax resident in a jurisdiction with which EU has agreed to automatically exchange information.

The Company shall be responsible for the collection and monitoring of the required information which shall be under the supervision of the Company's Compliance Officer.

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

7.6. Construction of an economic profile

(1) Irrespective of the customer's type (e.g. natural or legal entity, sole trader or partnership), the Company requests and obtains sufficient data and information regarding the customer's business activities.

(2) Without prejudice to the relevant provisions of section 7.4.1 of the Manual, the data and information that are collected before the establishment of the business relationship, with the aim of constructing the customer's economic profile and, as a minimum, include the following:

(a) the purpose and the reason for requesting the establishment of a business relationship;

(b) the anticipated business , the nature of the transactions,

(c) clear description of the main business/professional activities/operations.

(3) The data and information that are used for the construction of the customer's-legal person's economic profile include, inter alia, the name of the company, the country of its incorporation, the head offices address, the names and the identification information of the beneficial owners, Directors and authorised signatories, financial information, ownership structure of the group that the company may be a part of (country of incorporation of the parent company, subsidiary companies and associate companies, main activities and financial information). The said data and information are recorded in a separate form designed for this purpose which is retained in the customer's file along with all other documents as well as all internal records of meetings with the respective customer. The said form is updated regularly or

whenever new information emerges that needs to be added to the economic profile of the customer or alters existing information that makes up the economic profile of the customer.

Identical data and information with the above mentioned are obtained in the case of a customer-natural person, and in general, the same procedures with the above mentioned are followed.

(4) Transactions done for the customer are compared and evaluated against the activities/operations of the customer and the data and information kept for the customer's economic profile. Significant deviations are investigated and the findings are recorded in the respective customer's file.

(5) Information on the customer, are thoroughly examined so as to determine whether suspicions over money laundering or terrorist financing arise for the purposes of submitting an internal report to the compliance officer and then by the Compliance Officer's Report to the Unit for Combating Money Laundering.

(6) The Information regarding the Client's Economic Profile and Identification is collected by the Client's Vendor registration/customer registration Questionnaire.

7.7. Failure or refusal to submit information for the verification of customers' identity

(1) Failure or refusal by a customer to submit, before the establishment of a business relationship , the requisite data and information for the verification of his identity and the creation of his profile, without adequate justification, constitutes elements that may lead to the creation of a suspicion that the customer is involved in money laundering or terrorist financing activities. In such an event, the Company does not proceed with the establishment of the business relationship at the same time the compliance officer considers whether it is justified under the circumstances to submit a Compliance Officer's Report to the Unit for Combating Money Laundering.

(2) If, during the business relationship, a customer fails or refuses to submit, within a reasonable timeframe, the required verification data and information according to the Law and the Directive, the Company terminates the business relationship. At the same time examines whether it is justified under the circumstances to submit a report to Compliance Officer's Report to the Unit for Combating Money Laundering.

7.8. Customer's termination

The Company may terminate the business relationship with an existing client (for AML purposes or any other reason indicated below) at any time by giving ten (10) days written notice to the other Party or, without notice if the following occur:

If a Client fails or refuses to submit, within a reasonable timeframe (15) fifteen days, the required data and identification information for the updating of his/her identity and business profile and, as a consequence, the Company is unable to comply with the customer identification requirements set out in the Law and the Directive, then the Company will terminate the business relationship, while at the same time it should examine whether it is warranted under the circumstances to submit a report of suspicious transactions/activities.
It is given that in the case where the termination of the business relationship occurs due to any unlawful or suspicious actions/aspect identified in the client's activities/documents/information and/or transactions, a report shall be filed accordingly.

In addition to the aforesaid, if a client does not provide the Company with the requested information or supplementary documentation/information, the Company shall terminate the client according to Client Agreement.
In particular, during the business relationship established with clients, the Company's Compliance Department shall conduct on-going monitoring on the clients' profile, documentation and other related information and shall compare it with the actual trading activity, monetary transactions as described in the AML monitoring Policy and shall request from the Customer Support department to request any missing or outdated information from the relevant clients, assigning a timeframe/deadline to clients to provide the requested information. The timeframe shall be set based on the principles described in the above and shall be determined in accordance with the risk level posed by the client involved.

7.9. Simplified customer identification and due diligence procedures

(1) According to the Law, the Company, may apply simplified identification and due diligence measures provided that the Company ascertain that the business relationship present a lower degree of Money Laundering or Terrorist Financing occurring.

It is further provided that the Company is required to apply continuous monitoring of the business relationship, in order to be able to detect unusual or suspicious transactions.

(2) When assessing the risks of money laundering and terrorist financing relating to types of customers, geographic areas, and particular products, services, transactions or delivery channels, the Company shall take into account at least the factors of potentially lower risk situations set out in **APPENDIX V** of this Manual.

(3) In respect of the customers referred to in **APPENDIX V** of this Manual. It is provided that the Company collects sufficient information, so as to decide whether the customer can be exempted according to the provisions of the this section and **APPENDIX V** of the manual and the Company applies in respect of the aforesaid customers any other necessary Customer Identification and Measures mentioned in this manual.

(4) The Company does not consider that customers referred to in **APPENDIX V** of the Manual 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.

7.10. Enhanced Customer Identification and Due Diligence Procedures

(1) According to the Law the Company applies enhanced customer identification and due diligence procedures in addition to the measures referred to in Sections 7.1, 7.2.,7.3 and 7.4 when the Company has a transaction with physical person or a legal entity that is resident in a High Risk Third Country;

(2) According to the Law the Company applies enhanced customer identification and due diligence procedures in addition to the measures referred to in Sections 7.1, 7.2.,7.3 and 7.4 in other situations, that pose a high level of risk for money laundering or terrorist financing.

(3) When assessing the risks of money laundering and terrorist financing, the Company shall take into account at least the factors of potentially higher-risk situations set out in **APPENDIX VI** of this manual.

(4) The Company examines, as far as reasonably possible, the background check and shall increase the degree and nature of monitoring of the business relationship, in order to determine whether activities appear suspicious.

(5) According to the Law the Company applies the following enhanced customer identification and due diligence procedures in addition to the measures referred to in Sections 7.1, 7.2.,7.3 and 7.4 to the below Categories of Customers:

7.10.1. Non-exhaustive List of factors of potentially higher risk and enhanced due diligence measures

Without prejudice of the indicative factors of potentially higher risk of money laundering and terrorist financing as indicated in Appendix VI of this Manual and (b) enhanced due diligence measures stated in Appendix III of the Law and the Joint Guidelines.

If the Company concludes that the non-face-to-face business relationship or transaction as specified in paragraph 2(c) of Appendix III of the Law, presents higher risk of money laundering or terrorist financing, it should apply enhanced customer due diligence measures.
those of the EU Directive and the provisions of Annex II of the Law .

A direct confirmation of the establishment of a business relationship is obtained through direct personal contact, as well as, the true name, address and passport/identity card number of the customer, from a credit institution or a financial institution with which the customer cooperates, operating in a Member State or in a Third Country, which considered by the Company as lower risk, considering the requirements on combating money laundering are equivalent to those of the EU Directive and the provisions of Annex II of the Law (or a true copy of the confirmation).
Communication with the customer through at an address that the Company has previously verified from an independent and reliable sources, in the form of a registered letter (For example, such communication may take the form of a direct mailing of account opening documentation to him, which the customer shall return to the Company or the Company may send security codes required by the customer to access the accounts opened through the internet).

7.10.2. Politically Exposed Persons

(1) The Company adopts the following additional due diligence measures when it establishes a business relationship with a politically exposed person:

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

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

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

iv. The Company creates the profile of the customer by obtaining the information specified in subsection 7.6 of this manual. The details of the expected business and nature of activities of the customer forms the basis for the future monitoring of the client. The profile should be regularly reviewed and updated with new data and information. The Company is particularly cautious and most vigilant where its customers are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks.

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

vi. Without prejudice to the application, on a risk-sensitive basis, of the enhanced customer due diligence measures of section 7.10, where a politically exposed person is no longer entrusted with a prominent public function by a Member State or a third country, or with a prominent public function within the meaning of section 7.4.2.5(a) of this manual, the Company shall, for at least 12 months, be required to take into account the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to politically exposed person.

7.10.3. Customers from countries which inadequately apply Financial Action Task Force's recommendations or included in the EU Commission's List of high risk third countries regarding ML/TF

(1) The Company applies the following Enhanced Due Diligence Measures:

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

ii. Transactions with persons from the said countries, for which there is no apparent economic or visible lawful purpose, are further examined for the establishment of their economic, business or investment background and purpose. If a Company cannot be fully

satisfied as to the legitimacy of a transaction, then a suspicious transaction report is filed, according to Section 9.3 of this manual

iii. With the aim of implementing the above, the compliance officer consults the country assessment reports prepared by the FATF the other regional bodies that have been established and work on the principles of FATF [e.g. Moneyval Committee of the Council of Europe (www.coe.int/moneyval)] and the International Monetary Fund (www.imf.org). Based on the said reports, the compliance officer assesses the risk from transactions and business relationships with persons from various countries and decides of the countries that inadequately apply the FATF's recommendations. According to the aforesaid decision of the compliance officer, the Company applies, when deemed necessary, enhanced due diligence measures for identifying and monitoring relationship of persons from countries with significant shortcomings in their legal and administrative systems for the prevention of money laundering and terrorist financing.

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

The Company may accept as customers 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 described above for legal persons

7.11. Ongoing monitoring of accounts and transactions

The constant monitoring of the Client is a vital part and an imperative element in the effective controlling of the risk of Money Laundering and Terrorist Financing. Ongoing monitoring procedures assist the Company to update existing knowledge on its clients and detect any unusual or suspicious activities. 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.

Procedures:

The procedures and intensity of monitoring Clients' and examining transactions on the Client's level of risk shall include the following taking into account the principle of proportionality:

a) the identification of:
    - transactions which, as of their nature, may be associated with money laundering or terrorist financing

- unusual or suspicious business that are inconsistent with the economic profile of the Client for the purposes of further investigation.
- in case of any unusual or suspicious business, the head of the department providing the relevant investment and/or ancillary service as well as the Head of the Administration Department shall be responsible to communicate with the AMLCO

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

7.12. Monitoring Procedures as per Paragraph 26 of the Directive

The procedures and frequency of monitoring clients and examining clients' business are based on the level of risk and shall include the following:

- The Identification of:

a) high risk clients. The Company shall be able to produce detailed lists of high risk clients, so as to facilitate enhanced monitoring of as deemed necessary;

b) Business which, as of their nature, may be associated with money laundering or terrorist financing;

c) unusual or suspicious business that are inconsistent with the economic profile of the client for the purposes of further investigation;

d) in case of any unusual or suspicious business, the head of the department providing the relevant investment and/or ancillary service or any other person who identified the unusual or suspicious business shall be responsible to communicate with the Compliance/AML Officer.

- The investigation of unusual or business by the Compliance/AML Officer. The results of the investigations are recorded in a separate memo and kept in the file of the clients concerned.
- The monitoring of business transactions in relation to specific types of transactions and the economic profile, as well as by comparing periodically the actual movement with the expected turnover as declared at the establishment of the business relationship.

7.13. Screening system

The Company should buy and use automated screening systems which can assist in the detection and assessment of whether a client or potential client is subject to EU/UN and international sanctions, politically exposed person (PEP), convicted or suspected criminal. The Company must ensure that correct ML/TF risk classification performed on the basis of CDD measures before establishing a business relationship with a client, and on an ongoing basis.

The Company shall consider the following parameters in the selection process and when and how to be used:

(1) The screening system shall be appropriate to the nature, size and ML/TF risks of the Company. This should include well-documented policies and procedures.

(2) Screening should be performed before:

- the establishment of a business relationship;
- the provision of any services; and
- undertaking any transactions for a customer.

Thereafter, monitoring should be undertaken on an ongoing basis for customers and customers' related entities, directors and beneficial owners.

(3) The Company must ensure that the automated screening system is up to date and correct. Also ensure that there is a full understanding of the capabilities and limits of the screening system in order to apply extra measures whenever deemed necessary.

(4) The automated management information system should be tailored in line with Company's risk appetite, and perform regular reviews of the calibration and rules to ensure its effective operation.

(5) The Company should implement controls that require referral to relevant compliance staff prior to dealing with flagged persons.

8. Customer Acceptance Policy

8.1. Scope

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's KYC form. The AMLCO shall be responsible for applying all the provisions of the CAP. In this respect, the Head of the Administration Department shall also be assisting the AMLCO with the implementation of the CAP, as applicable. The Internal Auditor shall review and evaluate the adequate implementation of the CAP and its relevant provisions, at least annually.

8.2. General Principles of the CAP

The General Principles of the CAP are the following:

(a) the Company shall classify Clients into various risk categories and based on the risk perception decide on the acceptance criteria for each category of Client
(b) where the Client is a prospective Client, relationship must be opened only after the relevant due diligence and identification measures and procedures have been conducted, according to the principles and procedures set in Section 13 of the Manual
(c) all documents and data described in Section 13.5 of the Manual must be collected before accepting a new Client
(d) no reltioship shall be started in anonymous or fictitious names(s)
(e) no relatioship shall be started unless the prospective Client is approved by:
- the General Manager
- the AMLCO.

The Company has a CAP in place which is commensurate to the risks that the Company is willing to take—its risk appetite. Although the Company has a categorisation system in place:

- Low,
- Medium
- And High,

it only refuses to take on clients that are disqualified by the Law. In other words, the company is confident in its ability to manage and mitigate risks and is therefore willing to accept high-risk clients such as PEPs and clients from high-risk jurisdictions. On the other hand, sanctioned clients and countries, clients who have been convicted of serious crimes and so on are automatically rejected. In such cases, the CO of the company who is also the one who assesses risk levels decides whether to notify the Commission.

The CAP of the company consists of two parts. Firstly, the prospective client-persons whether natural or legal receives a questionnaire which they have to fill in and attach to it the required information. Once the company receives the above the CO conducts a check through the software and fills in Company's CAP and AML Checklist. The purpose of the form is to essentially make sure that all the necessary documentation, information and data have been received by the Company given the nature of the prospective business relationship and for the CO to place the client into a risk category (low, medium, high). As previously noted, the Company does not reject clients that are not eliminated based on the Law but instead applies the appropriate controls and mechanisms that the CO has designed for such cases which include EDD and close monitoring of accounts, transactions and activities to make sure that everything is in order. As far as the acceptance stages are concerned the Company might ask high-risk clients for additional information and documentation such as bank statements and tax declarations (certified by a reputable institution/practitioner).

All information obtained from the questionnaire and the CAP form are first processed in the software which determines its risk level always in relation to the nature of the business relationship and the services that Company will provide to the said client. However, the CO then

re-evaluates the risk level based on his assessment and may subsequently decide to alter the classification that has been assigned to a client by the software.

8.2.2 Documents/data collection (KYC) requirements

1. The documents/data obtained, for compliance with the Law, are the following forms:
   a) Original, or
   b) True copy of the original, where the certification is made by the Obliged Entity in cases where it establishes the customer's identity itself, once the original is presented thereto, or
   c) True copy of the original, where the certification is made by third parties, in cases where they establish the customer's identity, or
   d) True copy of the original, where the certification is made by a competent authority or person that, pursuant to the relevant provisions of the laws of their country, is responsible to certify the authenticity of documents or information. In this case the documents should be apostilled or notarised, or
   e) Provided that at least one of the procedures referred to in Paragraph 7.11.1 of this Manual is followed:
      i. Copy of the original, or
      ii. Data and information collected via electronic verification in accordance with the provisions of paragraph (2) below.

2. Performing an electronic verification:
   a) Electronic identity verification is carried out either directly by the Company or through a third party. Both the Company and the said third parties cumulatively satisfy the following conditions:
      i. the electronic databases kept by the third party or to which the third party or the Company has access are registered to and/or approved by the Data Protection Commissioner in order to safeguard personal data (or the corresponding competent authority in the country the said databases are kept).
      ii. electronic databases provide access to information referred to both present and past situations showing that the person really exists and providing both positive information (at least the customer's full name, address and date of birth) and negative information (e.g. committing of offences such as identity theft, inclusion in deceased persons records, inclusion in sanctions and restrictive measures' list by the Council of the European Union and the UN Security Council).
      iii. electronic databases include a wide range of sources with information from different time periods with real-time update and trigger alerts when important data alter.

iv. transparent procedures have been established allowing the 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 customer's identity verification
v. procedures have been established allowing the Company to record and save the information used and the result in relation to identity verification.

b) Information must come from two or more sources. The electronic verification procedure shall at least satisfy the following correlation standard:
   i. identification of the customer's full name and current address from one source, and
   ii. identification of the customer's full name and either his current address or date of birth from a second source.
c) For purposes of carrying out the electronic verification, the Company shall establish procedures in order to satisfy the completeness, validity and reliability of the information to which it has access. It is provided that the verification procedure shall include a search of both positive and negative information.
d) It is provided that the Company evaluates the results in order the conditions of the Law to be satisfied. The Obliged Entity establishes mechanisms for the carrying out of quality controls in order to assess the quality of the information on which it intends to rely.

8.2.3 Individuals / Natural persons:

Before establishing a business relationship with an Individual / Natural person who wishes to be accepted as the Company's client the Company obtains the following identification information in order to ascertain the true identity of the natural person:

i. True name and/or names as stated on the official identity card or passport,

ii. Full permanent address, including postal code,

iii. Telephone (home and mobile) and fax numbers (if any),

iv. E-mail address,

v. Date and place of birth,

vi. Nationality

vii. Number of Passport and Country of Issue

viii. Details of the profession and other occupations of the applicant, including the name of employer/business organization

ix. Information to enable the Company to construct an economic profile of the client

The above information is collected by means of completing and signing the Client KYC Form for UBOs

For the verification of the identity of the aforesaid person the Company obtains the following documents depending on the risk classification of the Customer:

For applicants residing in EU such person should provide the Company with a copy (original or certified true copy) of passport or other forms of official document confirming his/her identity).

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

In rare and exceptional cases, clients providing only one form of official ID will be accepted (if no other form of official ID is available).

The following must always appear on the copies of the documents obtained:

i. Passport number and/or ID number

ii. Issuing date and country

iii. Applicant's date of birth

iv. Applicant's photo

v. Validity date (if any)

If in doubt for the genuineness of any document (passport, identity card or any other documentary evidence) it is common practice to seek verification of identity from an Embassy or the consulate of the issuing country or a reputable credit or financial institution situated in the applicant's country of residence.

In case where the applicant was introduced by a reliable staff member or by another existing reliable client who is personally known to the Board of Directors, details of such introduction shall be kept in the prospective client file. Bank reference is also reliable source of recommendations and required where applicable.

It is important that the applicant's permanent address is also verified using one of the following ways:

i. The original or certified copy of a recent (up to 6 months) utility bill, bank statement, local authority tax bill bearing the full address (including the postal code where available) and name of the applicant as stated in the Client's KYC Questionnaire

ii. Visit the place of residence (in such case, the Company's officer who carries out the visit should prepare a memo which is retained in the customer's file)

As mentioned above the documentation collected for Individuals / Natural persons include the following:

i. International Passport or ID.

ii. Residence confirmation (not older than 6 months)

iii. Documentation evidencing the source of funds (where applicable)

iv. Automated scanning via Sanctions and PEP lists (WORLD-CHECK)

The Company hereby reserves its right to collect any additional documentation and apply any additional Enhanced Due Diligence from each customer if such request/measure is justified by the customers unique circumstances.

8.2.4 Legal Entity/ Legal Person:

Before establishing any business relationship with an applicant - Legal Entity/Legal Person the Company establishes that the natural person appearing to act on their behalf is appropriately authorized to do so. Furthermore, the Company should ascertain the true identity of the legal entity by obtaining the following information and documents:

i. Country and Number of Registration

ii. The full legal name (registered corporate name)

iii. The full address of the registered office and mailing/business address

iv. Telephone and fax numbers and email address

v. The individuals that are duly authorized to operate the account and to act on the behalf of the legal person

vi. The beneficial owners of private companies and public companies that are not listed in a regulated market of the European Economic Area country or a 3rd country with equivalent disclosure and transparency requirements

vii. The registered shareholders that act as nominees of the beneficial owners

viii. The economic profile of the legal person.

The above information is collected by means of completing and signing the Client KYC Questionnaire for Legal Entity which is compulsory for every applicant.

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

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

ii. certificate of registered office,

iii. certificate of Directors and secretary,

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

v. Memorandum and Articles of Association of the legal person,

vi. 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,

vii. documents and data for the verification, according to the provisions of the present Directive, the identity of the persons that are authorised by the legal as well as the registered shareholders and beneficial owners of the legal person.

viii. Automated scanning via Sanctions and PEP lists (WORLD-CHECK - based automated application) for directors, authorised signatories, shareholders and ultimate beneficiaries

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

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

The Company may establish and maintain business relationships with legal persons who carry out regulated services and activities which are incorporated and/or operating in countries of the European Economic Area or an Equivalent Country, provided that:

i. the said persons possess the necessary license or authorization from a competent supervisory/regulatory authority of the country of their incorporation and operation to provide the said services, and

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

In case of a third country other than those mentioned above, the Company requests and obtains, documentation for the identification and verification of persons, including the beneficial owners, the following:

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

ii. Adequate documentation and sufficient information in order to fully understand the control structure and management of the business activities as well as the nature of the services and activities provided by the customer.

The Company can collect copies of the original of the aforesaid documents for Regulated Companies with whom the Company does not come to immediate and personal contact provided that it will apply at least one of the Enhanced Due Diligence Measures that are mentioned in 0(**Error! Reference source not found.**) of this Risk Management and Procedures Manual.

The Company hereby reserves its right to collect any additional documentation and apply any additional Enhanced Due Diligence from each Regulated Company if such request/measure is justified by the customer unique circumstances.

8.2.5 Categories of customers who are not acceptable for establishing a business relationship or an execution of an occasional transaction;

The Company has decided that the risk associated with certain groups of customers is unacceptably high and has therefore decided to preclude such customers from establishing a business relationship with the Company. Apart from the requirements of the Law and the Directive and the Risk Management and Procedures Manual, the Company, as part of its Risk Appetite Assessment, has included in this category other types of customers based on their Money Laundering / Terrorism Financing risk. Specifically, the Company prohibits the establishment of a business relationship with a person (physical and/or legal), that:

i. Clients failing or refusing to submit the required data and information for the verification of his /her identity or address and the creation of his/her economic profile.

ii. Clients whose identification is not possible to check based on the provided information

iii. Clients - residents of the countries where the Company is not authorized to offer the service due to local regulations and/or restrictions

iv. Clients who are included in the EU/UN Sanctions Lists

v. Any other client who given his circumstances may be considered of an unacceptable risk level by the Company. Factors to be considered include the applicant's background, type and nature of the applicant's business activities, country of origin, the anticipated level and nature of the business transactions, as well as the expected source and origin of the funds.

8.3. Criteria for Risk Based Categorization of Customers

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

8.3.1 Low Risk Customers

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

- Business entities covered by the EU Directive
- Business entities carrying out one or more of the financial business activities as these are defined by the Law and which is situated in a country outside the EEA, which:

- in accordance with a decision of the Advisory Authority, imposes requirements equivalent to those laid down by the EU Directive and
- it is under supervision for compliance with those requirements
- listed companies whose securities are admitted to trading on a Regulated Market in a country of the EEA or in a third country which is subject to disclosure requirements consistent with community legislation
- domestic public authorities of countries of the EEA.

The Company does not classify as low risk the aforesaid clients if there is information suggesting that the risk of money laundering or terrorist financing associated with those clients may not be low and provided that there is no other factors according to which the Company is required either by the Law, the Directives and this Risk Management and Procedures Manual to classify them differently.

It is further provided that the Company is required to apply continuous monitoring to the aforesaid persons.

8.3.2 Normal Risk Customers

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

• any Client who does not fall under the 'low risk Clients' or 'high risk Clients' categories set in Sections 8.3.1 and 8.3.3, respectively.

8.3.3 High Risk Customers

The following categories of customers are designated by default either by the Law or the Directive as high risk and, therefore, the Company is obliged, apart from normal customer identification and due diligence measures set out in the Law and the Directive, to perform enhanced due diligence measures, as well as on-going monitoring of accounts and transactions:

i. Accounts for Politically Exposed Persons ("PEPs")
ii. Clients residing/incorporated in high risk jurisdictions regarding ML/TF based on FATF public statements and EU Commission's list regarding high risk third countries regarding ML/TF

Without prejudice of the indicative factors of potentially higher risk of money laundering and terrorist financing and enhanced due diligence measures stated in Appendix III of the Law and the Joint Guidelines as indicated in **APPENDIX VI** of this Manual, the following indicative factors

and measures should be taken into account by the Company during the risk based approach and the application of enhanced customer due diligence measures:

1. Clients whose own shares or those of their parent companies (if any) have been issued in bearer form
2. Shares held in Trust
3. PEP(s)
4. Clients from countries which inadequately apply FATF's recommendations or included in the EU Commission's list of high risk third countries in relation to ML/TF
5. any other Clients that their nature entail a higher risk of money laundering or terrorist financing
6. any other Client determined by the Company itself to be classified as such.

When assessing the risks of money laundering and terrorist financing, the Company shall take into account at least the factors of potentially higher-risk situations set out in **APPENDIX VI** of this manual in order to assess whether the person with whom will establish a business relationship with will be categorized as high risk.

In addition, the Company shall take into account the Risk Factors, when assessing the money laundering and terrorist financing risk associated with business relationships and occasional transactions.

8.4. Updates

The Company shall review the CAP on an annual basis to ensure that it stays current with all the requirements of the Law and the Directives and the Company shall update it whenever there are amendments to the Law and the Directive.

9. Recognition and Reporting of Suspicious Transactions/Activities

9.1. Reporting of suspicious transactions

(1) The Company shall refrain from carrying out transactions which knows or suspects that are related with money laundering or terrorist financing before they inform the Unit of their suspicion in accordance with sections 9.1(3) and 9.1 (4) of this manual;

(2) It is provided that, if it is impossible to refrain from carrying out the transaction or is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist

financing operation, the persons engaged in financial or other business activities, must inform the Unit immediately afterwards.

(3) A person who-

(a) knows or reasonably suspects that another person is engaged in laundering or financing of terrorism offences, and

(b) the information on which that knowledge or reasonable suspicion is based, comes to his attention in the course of his trade, profession, business or employment, shall commit an offence if he does not disclose the said information to the Unit as soon as is reasonably practicable after it comes to his attention.

(c) The existence of reasonable explanation or justification for the non-disclosure of the abovementioned information shall constitute defence.

(4) The Company shall apply the following internal reporting procedures:

(a) Appoint a senior staff member who has the ability, the knowledge and the expertise on financial or other business activities, according to each case, as a Anti money laundering compliance officer to whom a report is to be made about any information or other matter which comes to the attention of the person handling financial or other business activities and which, in the opinion of the person handling that business, proves or crates suspicion that another person is engaged in a money laundering offence or terrorist financing.

(b) requiring that, any such report to be considered in the light of all other relevant information by the money laundering compliance officer, for the purpose of determining whether or not the information or other matter contained in the report proves this fact or creates such a suspicion.

(c) allowing the anti money laundering compliance officer in accordance with paragraph (b) above to have direct and timely access to other information, data and documents which may be of assistance to him and which is available to the person engaged in financial or other business activities.

(d) When they know or have reasonable suspicions that transfer of funds regardless of its amount constitutes proceeds from criminal activities or is related with terrorist financing, they ascertain that such information is transmitted to the Unit immediately on their own initiative by submitting the relevant report and providing any additional information requested by the Unit.

(5) Without prejudice to the provisions of subsections 9.1(1)(2) of this manual , the Company, in cases where there is an attempt of executing transactions which knows or suspects that are related to money laundering or terrorist financing, reports, through the compliance officer its suspicion to the Commission in accordance with paragraph 5.1(g).

9.2. Suspicious transactions

(1) The definition of a suspicious transaction as well as the types of suspicious transactions which may be used for money laundering and terrorist financing are almost unlimited. A suspicious transaction will often be one which is inconsistent with a customer'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 customer. The Company ensures that maintains adequate information and knows enough about its customers' activities in order to recognise on time that a business or a series of transactions is unusual or suspicious.

(2) A list containing examples of what might constitute suspicious transactions/activities related to money laundering and terrorist financing is attached to the **APPENDIX VIII**. The said list is not exhaustive nor includes all types of transactions that may be used, nevertheless it can assist the Company and its employees 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 **APPENDIX VII** 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.

9.3. Compliance officer's report to the Commission

(1) All the reports of the compliance officer of paragraph 5.1(g).are send or submitted the Commission**.**

(2) After the submission of a suspicious report of paragraph 5.1(g),the Company may subsequently wish to terminate its relationship with the customer concerned for risk avoidance reasons. In such an event, the Company exercises particular caution, not to alert the customer concerned that a suspicious report has been submitted.

In Exercising Particular caution as described above Company shall do the following:

(3) The Company, its directors and employees shall not disclose to the customer concerned or to other third persons the fact that information is being, will be or has been transmitted in the Commission that a money laundering or terrorist financing analysis is being, or may be, carried out.

Is prohibited to any person to make any disclosure which may impede or prejudice interrogations and investigations that are carried out in respect of prescribed offences or the ascertainment of proceeds of proceeds, knowing or suspecting that the said interrogation and investigation are taking place

(4) After submitting the suspicious report of paragraph 5.1(g), the Company adheres to any instructions given by the Commission and, in particular, as to whether or not to continue or suspend a particular business.

9.4. Submission of information to the Commission

The Company ensures that in the case of a suspicious transaction investigation by the Commission, will be able to provide without delay the following information:

(a) the identity of the person and entity;

(b) the identity of the beneficial owners;

(c) the identity of the persons authorised to manage the entity;

(d) POA holder's if any for the entity

9.5. United Nations ('UN') and European Union ('EU') Sanctions Regimes

(1) The Company shall design and implement measures and procedures for the detection of actions that are in breach or may potentially be in breach of the provisions of the United Nations Security Council Resolutions or Decisions ('Sanctions') or/and the European Union Council Decisions and Regulations ('Restrictive Measures'), as provided for in the Sanctions Law.

(2) Where the Company intends to take an action, which falls within those cases that may be approved under the provisions of the Sanctions or Restrictive Measures, the Company shall submit, prior to taking the said action, through its compliance officer.

(3) The Company shall establish a procedures manual for the measures and procedures for the detection of actions that are in breach or may potentially be in breach of the provisions of the Sanctions and Restrictive Measures. The Company may establish a separate Sanction Policy to comply with the said requirement.

10. Record Keeping Requirements

10.1. Record Keeping and Time Period of Retaining Documents/Data

(1) The Company keeps record of the documents/data that are specified in the present manual, including those referred to in subsection 5.1(l) and sections 7.4, 7.8, 7.10 **Error! R eference source not found.** and on the CAP on Section 8, such records are also referred to below:

(a) Copies of the Documents and Data that they are required for compliance with the Customer Due Diligence Measures in this manual;

(b) The relevant correspondence documents with the customers and any other persons with whom a business relationship is maintained

(2) The documents/data of subparagraph (1), are kept for a period of at least five (5) years, which is calculated after the execution of an occasional transaction or the termination of the business relationship.

10.2. Format of Records

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

(2) When the Company establishes a documents/data retention policy, takes into consideration the requirements of the Law and the present Directive and the potential needs of the Commission.

11. Employees' Obligations, Education and Training

11.1. Employees' obligations

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

(2) The employees cooperate and report, without delay, according to paragraph 5.1(e) anything that comes to their attention in relation to transactions for which there is a slight suspicion that are related to money laundering or terrorist financing.

(3) The Company's employees fulfil their legal obligation to report their suspicions regarding money laundering and terrorist financing if they follow the reporting procedure for such disclosures pursuant to this manual, and these disclosures shall have the same effect as disclosures or intended disclosures the Unit.

11.2. Employees' Education and Training Program

(1) The Company ensures that its employees are fully aware of their legal obligations according to the Law and the present Directive, by introducing a complete employee's education and training program.

(2) The timing and content of the training provided to the employees of the various departments is adjusted according to the needs of the Company. Regular training shall be conducted, at least on an annual basis, to ensure that staff and Board of Directors are aware of the ML/TF risks posed by its activities and the policies, controls and procedures that the Company has in place. In addition, the frequency of the training can be more regular based on to the amendments of legal and/or regulatory requirements, employees' duties as well as any other changes in the financial system of the country.

(3) The training program aims at educating employees on the latest developments in the prevention of money laundering and terrorist financing, including the practical methods and trends used for this purpose.

(4) The AMLCO is responsible for determining whether the staff has the necessary knowledge for the purpose of preventing ML/TF or whether further training is required. The training program has a different structure for new employees, existing employees and for different departments/positions of the Company and level of responsibility who may face different ML/TF risks ensuring that staff is equipped with sufficient knowledge
allowing them to identify suspicious transactions and activities and according to the services that they provide.

(5) When setting up a staff training program, the Company should consider:

- which staff require training;
- what is the content of the training provided; (e.g. legal framework, clent 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 Company.

(6) Furthermore, training can take many forms and may include:
• face-to-face training seminars (in-house 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.

(7) As a general rule, 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. Apart from the mandatory training, the Company should establish mechanisms to facilitate prompt updates on key trends, emerging risks, potential ML/TF activities/risks, legislative changes and internal policies, controls and procedures and must ensure that such updates are communicated in a timely manner to staff.

(8) Moreover, the Company should put in place mechanisms to measure and assess the adequacy and effectiveness of staff AML/CFT training, with reference to the results, i.e. inclusion of tests following completion of the training with minimum pass rates. In the event that the employee will not pass the relevant test twice, then a warning notice shall be communicated to him/her and another test shall be provided from the Company within one month from the date that failed the last test. If the employee does not pass the third test, then shall be dismissed from the Company which is derived based on the contractual agreement between the employee and the Company.

11.3. Board of Directors and Senior Management

(1) The Board of Directors (BoD) and Senior Management of the Company must put in place an AML/CFT compliance programme that not only ensures compliance with the relevant legislation, but where necessary includes further action to mitigate any specific and unique vulnerability that the regulated entity might have to ML/TF.

(2) In general, the BoD and Senior Management should:

- approve the mandatory annual training programme prepared by the AMLCO,
- ensure that it receives adequate management information on the implementation of the Company's AML/CFT training programme,
- 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) In general, the Company shall:

i. have documented and on-going training plan in place to ensure appropriate levels of AML/CFT training are provided to the BoD and all staff involved in the conduct of the business;
ii. Training content is reviewed and updated on a regular basis to ensure it remains current and appropriate and the material is approved by senior management;
iii. Enhanced training is provided to senior management and staff in key AML/CFT roles to endure their knowledge remains adequate and up-to-date;
iv. Training records are maintained.

12. APPENDIX I - Internal Suspicion Report for Money Laundering and Terrorist Financing

INFORMER'S DETAILS

Name: ..... Tel: .....

Department: ..... Fax: .....

Position: .....

CLIENT'S DETAILS

Name: .....

Address: .....

.....

..... Date of Birth: .....

Tel: ..... Occupation: .....

Fax: .....

Details of Employer: .....

Passport No.: ..... Nationality: .....

ID Card No.: .....

Other ID Details: .....……

INFORMATION/SUSPICION

Brief description of activities/transaction: .... ……

....

..... ……

Reason(s) for suspicion:

.....

.... ……

Informer's Signature Date

…….…

..... …..

FOR COMPLIANCE OFFICER'S USE

Date Received: ..... Time Received: ..... Ref.....

Reported to the Commission: Yes/No …….. Date Reported: ..... Ref.....

13. APPENDIX II – Compliance Officer's Report to the Unit for Combating Money Laundering (STR)

I. GENERAL INFORMATION

Company's Name: .....

Address of the Customer: .....

.....

Date when a business relationship established or

II. DETAILS OF NATURAL PERSON(S) AND/OR LEGAL ENTITY(IES) INVOLVED IN THE SUSPICIOUS TRANSACTION(S)

(A) NATURAL PERSONS

	Beneficial owner(s)	Authorized signatory(ies)
Name(s):	.....	.....
	.....	.....
Residential address(es):	.....	.....
	.....	.....
	.....	.....
	.....	.....
Business address(es):	.....	.....
	.....	.....
	.....	.....
Occupation and Employer:	.....	.....
	.....	.....
	.....	.....
Date and place of birth:	.....	.....
	.....	.....
	.....	.....
	.....	.....
Nationality and passport number:	.....	.....
	.....	.....
	.....	.....

....

(B) LEGAL ENTITIES

Legal entity's name, country and date of incorporation: .....
.....
.....

Business address: .....
.....
.....

Main activities: .....
.....
.....

	Name	Nationality and passport number	Date of birth	Residential address	Occupation and employer's details
Registered Shareholder(s)	1. ..... 2. ..... 3.	....	....	....	....
Beneficial Owner(s) (if different from above)	1. ..... 2. ..... 3.	....	....	....	....
Directors	1. ..... 2. ..... 3. ..... 4.	....	....	....	....
Authorized signatory(ies)	1. ..... 2. ..... 3.	....	....	....	....

III. DETAILS OF SUSPICIOUS ACTIVITIES

Details of suspicious activities should be given

1. .....
   .....
   .....
   .....
   .....
2. .....
   .....
   .....
   .....
   .....
3. .....
   .....
   .....
   .....
   .....

4. Knowledge/suspicion of money laundering or terrorist financing (please explain, as fully as possible the knowledge or suspicion connected with money laundering or terrorist financing)

   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....

5. Other information – Other services provided to the customer(s)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Compliance Officer's Signature Date

…….....……..... …….....

14. APPENDIX III - Internal Evaluation Report for Money Laundering and Terrorist Financing

Reference: ..... Client's Details: .....

Informer: ..... Department: .....

INQUIRIES UNDERTAKEN (Brief Description)

.....

.....

.....

ATTACHED DOCUMENTS

....

....

....

COMPLIANCE OFFICER'S DECISION

.....

.....

FILE NUMBER .....

COMPLIANCE OFFICER'S SIGNATURE DATE

....

15. APPENDIX IV – List of Risk Variables

Indicative list of risk variables that the Company shall consider when determining to what extent to apply customer due diligence measures in accordance with Section 7.4.1(10).

I.the regularity or duration of the business relationship.

16. APPENDIX V – List of Factors of Potentially Lower Risk

Indicative list of factors and types of evidence of potentially lower risk referred to in Section 7.8(2) of this manual.

(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) Geographical risk factors:

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

17. APPENDIX VI – List of Factors of Potentially Higher Risk

Indicative list of factors and types of evidence of potentially higher risk referred to in Section 7.10(3) of this manual.

(1) Customer risk factors:

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

(b) customers that are resident in geographical areas of higher risk as set out in point (3);

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

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

(e) businesses that are cash-intensive;

(f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

(2) Geographical risk factors:

(a) Without prejudice to Section 7.10(1), 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) third 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.

18. APPENDIX VII – Examples of suspicious Transactions / Activities Related to Money Laundering and Terrorist Financing

A. MONEY LAUNDERING

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

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

3. A customer is reluctant to provide complete information when establishes a business relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with Companys, names of its officers and directors, or information on its business location. The customer usually provides minimum or misleading information that is difficult or expensive for the Company to verify.

4. A customer provides unusual or suspicious identification documents that cannot be readily verified.

5. A customer's home/business telephone is disconnected.

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

7. A customer who has been introduced by a foreign Company, or by a third person whose countries or geographical areas of origin do not apply or they apply inadequately FATF's recommendations on money laundering and terrorist financing.

8. The stated occupation of the customer is not commensurate with the level or size of the executed transactions.

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

10. 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.

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

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

13. Changes the performance and the behavior of the employees of the Company.

B. TERRORIST FINANCING

1. Sources and methods

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

i. collection of membership dues and/or subscriptions,

ii. sale of books and other publications,

iii. cultural and social events,

iv. donations,

v. community solicitations and fund raising appeals.

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

2. Non-profit organizations

Non–profit and charitable organizations 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 organizations can be made in the following ways:

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

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

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

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

19. APPENDIX VIII - Definitions

For the purposes of this Manual the following terms shall have the meaning assigned to them here unless prescribed differently by the context:

Advisory Authority	means the Advisory Authority for Combating Money Laundering and Terrorist Financing
beneficial owner	the natural person who ultimately owns or controls a corporate entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that corporate entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with European Union law or subject to equivalent international standards which ensure adequate transparency of ownership information.. The beneficial owner shall at least include:

	(a) In the case of corporate entities: I. the natural person or natural persons, who ultimately own or control a legal entity through direct or indirect ownership or control of a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, a percentage of 25% plus one share be deemed sufficient to meet this criterion; II. the natural person or natural persons, who otherwise exercise control over the management of a legal entity. (b) In the case of legal entities, such as foundations and legal arrangements, such as trusts, which administer and distribute funds: (i) the settlor; (ii) the trustee or commissioner; (iii) the protector, if any; (iv) the beneficiary, or where the individual benefiting from the legal arrangement or legal entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates; (v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means c) in the case of legal entities, such as foundations, and legal arrangements similar to trusts, the natural person holding equivalent or similar positions to the person referred to in paragraph (b) above

Board of Directors	means the board of directors of the Financial Company;
Company	means a company of limited liability by shares, established under Company Law or a company established in another member state under the law applicable in its place of establishment or a company established under the Cooperative Societies Law; In this case the Company (Company) is ACU SA
Compliance officer	means the person referred to in Section 5 of this manual
countries of the European Economic Area-EEA	means Member State of the European Union or other contracting state which is a party to the agreement for the European Economic Area signed in Porto on the 2nd of May 1992 and was adjusted by the Protocol signed in Bruxelles on the 17th of May 1993, as amended
EU Directive	Means the Directive (EU) 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 as updated and amended from time to time
Administrative Services	means any of the services, in the Law the companies providing administrative services and related matters.
Law	means the Prevention and Suppression of Money Laundering Activities Law
Manual	Means the Risk Management and Procedures Manual (this manual), according to the EU Directive

MOKAS or Unit	means the Unit for Combating Money Laundering established according to section 54 of the Prevention and Suppression of Money Laundering Activities Law;
money laundering and terrorist financing offences	means the money laundering offences and terrorist financing offences defined in the Law.
Occasional Transaction	Means any transaction with the exclusion of any transaction carried out in the duration of a business relationship
Politically Exposed Persons or PEPs	Means the natural persons who are or have been entrusted with prominent public functions in the country or in other Country and their immediate family members or close associates of such persons for further information please refer to section 7.4.2.5(3)
Country	Company domiciled in that country
Shell Bank	means a credit institution or financial institution, or an institution that carries out activities equivalent to those carried out by credit institutions and financial institutions, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.
Third country	means a country not a member of the European Union or contracting party to the agreement of the European Economic Area signed in Porto on the 2nd of May 1992 and was adjusted with the Protocol signed in Brussels on 17 May 1993, as amended.

20. APPENDIX IX - FATCA Definitions

FATCA	The Foreign Account Tax Compliance Act (FATCA) of the Internal Revenue Code. It represents the US Treasury Department's efforts to prevent US taxpayers who hold financial assets in non-US financial institutions (foreign financial institutions or FFIs) and other offshore vehicles from avoiding their US tax obligations. The intent behind the law is for foreign financial institutions (FFIs) to identify and report to the IRS US persons holding assets abroad. In order to comply with the rules, FFIs are required to comply with intergovernmental agreements (IGAs) entered into by US and the Republic of Germany. Failure to enter into an agreement or provide required documentation will result in the imposition of a 30% withholding tax on certain payments made to such customers and counter-parties.
Foreign financial institution (FFI)	An FFI is defined as any financial institution that is a foreign entity, other than a financial institution organized under the laws of a possession of the United States. Financial institution means any entity that: I. accepts deposits or other similar investments of funds in the ordinary course of a banking or similar business (Depository Institution); II. holds, as a substantial portion of its business, financial assets for the benefit of one or more other persons (Custodial Institution); III. primarily conducts trading in money market instruments, foreign currency, foreign exchange interest rate, and index instruments, transferable securities or commodity futures; individual or collective portfolio management; or investing, administering or managing funds, money or

	financial assets on behalf of other persons (Investment Entity);
Indication of U.S Status or U.S Indicia	U.S. Final Regulations lists seven indicia of U.S. status: • U.S. citizenship or lawful permanent resident (green card) status; • A U.S. birthplace; • A U.S. residence address or a U.S. correspondence address (including a U.S. P.O. box); • A U.S. telephone number (regardless of whether such number is the only telephone number associated with the account holder) Standing instructions to pay any amounts from the account to an account maintained in the U.S.; • An "in care of" address or a "hold mail" address that is the sole address with respect to the client; or • A power of attorney or signatory authority granted to a person with a U.S. address.
Tax Identification Number	A Taxpayer Identification Number (TIN) is an identification number used by the Internal Revenue Service (IRS) in the administration of tax laws.
US-Reportable clients	A client that has U.S. Indicia Status

21. APPENDIX X – Employees Confirmation of Money Laundering Awareness

Name: _____

I confirm that I have read and understood the Company's documented money laundering policies and procedures that are included in the AML/CFT Risk Management and Procedures Manual and confirm that I will fully comply with these policies and procedures.

As a result of reading these procedures and any other training / information received, I confirm that I am aware of:

1 The Company's AML/CFT Risk Management and Procedures Manual

2 The identity of the Company's Money Laundering Compliance Officer (CO) – will be appointed

3 I also confirm that I have been given training in how to recognize and deal with transactions that may be related to money laundering,

_____
Signature

Name Surname:

Position:

Date:

22. APPENDIX XI - True Translation Form

I, FULL LEGAL NAME, hereby certify that I reviewed and translated the attached documents. (Please provide the name of the documents and attach the Documents as an Appendix to this Translation Form) I further certify that the English translation of the LANGUAGE document appears, to the best of my abilities, to be true, accurate, exact and full. I further certify that I am competent in both English and the (Provide the LANGUAGE) that I had render and certified such translation.

For and on Behalf of ACU SA

_____
Name Surname
Position

Signed this ___ day of _____ 20___

23. APPENDIX XII – Phone Verification Template

Phone verification for Individuals / Natural persons

Client's information	To be filled in next column	
Date:	Enter date of the conversation	
Full name:	"Confirmed as per registered data (**yes/no**)"	
Address:	"Confirmed as per registered data (**yes/no**)"	
ID/Passport number	Please enter number confirmed by the client	
Phone number registered:	"Confirmed as per registered data (**yes/no**)"	
Land Line called:	Please enter number called	
Comment:	If any	

Phone verification for Legal Entities

Client's information	To be filled in next column	
Date:	Enter date of the conversation	
Full name (Company):	"Confirmed as per registered data (**yes/no**)"	
Full name (Signatory / Authorized person):	"Confirmed as per registered data (**yes/no**)"	
Incorporation Number:	"Confirmed as per registered data (**yes/no**)"	
Year & Country of Incorporation:	"Confirmed as per registered data (**yes/no**)"	
Registered Address:	"Confirmed as per registered data (**yes/no**)"	
Names of Directors & Shareholders:	"Confirmed as per registered data (**yes/no**)"	
Services as per MAA:	"Confirmed as per registered data (**yes/no**)"	
Phone number registered:	"Confirmed as per registered data (**yes/no**)"	
Land Line called:	Please enter number called	
Comment :	If any	