

PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

Plotio Global Financial Limited

Procedures to be followed for the prevention of
Money Laundering and Terrorist Financing

Prepared January 2019

Executive Overview

“Money laundering” is an issue that many organizations faces, for example, financial institutions have been subject to legal and regulatory requirements in relation to money laundering for a number of years. The need to understand and manage money laundering and the risks it can present to an organization has never been greater, not only from a legal perspective but also to protect a firm’s reputation.

These procedures are designed to facilitate and to ensure the recognition and reporting of suspicious transactions through the strict implementation of the know-your-customer principle and the maintenance of adequate record keeping procedures should a customer come under investigation.

Scope

This definition deals with the general aspects of money laundering but the term ‘money laundering’ will often be used in a broader sense to include terrorist financing. Whilst terrorists will use the same general process to move money around and hide it from the authorities it should be remembered that terrorist funds are not always derived from criminal activity and can be derived from legitimately earned funds.

For the purpose of this policy the term ‘money laundering’ will include terrorist financing unless otherwise stated.

When money laundering is identified or suspected it is rarely the case that it can be categorized with any degree of certainty without further investigation by the authorities.

It is difficult to be specific about the risks that an organisation may face from money laundering, as money laundering can be a diverse and complex process. However, there are a number of factors that will assist in determining the levels and types of risk that an organisation may face from money laundering:

- ✓ Type of organisation / business
- ✓ Products / services produced / provided
- ✓ Geographical locations of the business and trading activity
- ✓ Methods of payment / funding

The risk from legal or regulatory action is much greater for businesses that undertake ‘regulated activity’ but it should be remembered that most of the statutory money laundering offences apply to everyone and therefore all organizations and their employees are at risk from legal proceedings if they become involved in money laundering.

Reputational damage is a risk that can result from involvement in money laundering activity and organizations with strong brand names could be particularly at risk. News of high profile money laundering investigations can result in a loss of confidence by customers and a subsequent fall in market value.

Anti-money laundering requirements

There are six key anti-money laundering requirements that are specific to "regulated activity". These provides a useful approach for the Company to consider when looking at how to manage the money laundering risk.

- ✓ Customer identification procedures,
- ✓ Record keeping procedures in relation to customer's identity and their transactions,
- ✓ Procedures of internal reporting to the Compliance and AMLO appointed to receive and consider information that give rise to knowledge or suspicion that a customer is engaged in money laundering activities,
- ✓ Other internal control and communication procedures for the purpose of forestalling and preventing money laundering,
- ✓ Measures for making employees aware of the above procedures to prevent money laundering and of the legislation relating to money laundering; and Provision of training to their employees in the recognition and handling of transactions suspected to be associated with money laundering and suspicious transactions.

Responsibilities of the Board of Directors

The responsibilities of the Board in relation to the prevention of money laundering and terrorist financing include the following:

(a) to determine, record and approve the general policy principles of the Company in relation to the prevention of money laundering and terrorist financing and communicate them to the AMLO

(b) to appoint the AMLO and, where is necessary, assistant AMLOs and determine their duties and responsibilities, which are recorded in this Manual

(c) to approve the Manual

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

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

(f) to ensure that all employees are aware of the person who has been assigned the duties of the AMLO, as well as his assistants (if any), to whom they report, any information concerning transactions and activities for which they have knowledge or suspicion that might be related to money laundering and terrorist financing

(g) to establish a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the AMLO, either

directly or through his assistants, if any, and notifies accordingly the AMLO for its explicit prescription in the Manual

(h) to ensure that the AMLO has sufficient resources, including competent staff and technological equipments, for the effective discharge of his duties

(i) to assess and approve the AMLO's Annual Report and take all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the abovementioned report

Obligations of the Internal Audit Department

The following obligations of the Internal Auditor are addressed specifically for the prevention of money laundering and terrorist financing:

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

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

Internal controls and procedures: AMLO

The Compliance officer is responsible for all issues relating to money laundering compliance and reporting. In "regulated activity" this person is referred to as the Anti-Money Laundering Officer (AMLO).

The AMLO is appointed by the Board of Directors and can be removed by them. The AMLO is sufficiently senior to command the necessary authority, and also has the position of the Compliance officer. The Company when needed may appoint other Deputy Compliance & Anti-Money Laundering Officer who will assist the AMLO in his/her work.

Deputies can obtain the copies of the originals provided by the Clients and carry out independent compliance and anti-money laundering inquiries with the clients but the approval and acceptance of the client lies on the decision of the Managing Director. A report is submitted to the Managing Director regarding each client, by the AMLO. The AMLO may reject the proposal for acceptance of the client. But in this case the AMLO has to inform the Board of directors about the reason of rejection.

The AMLO has the following duties and responsibilities:

- ✓ Prepares the internal procedures manual for the prevention of money laundering and terrorist financing and describes and designates the responsibility borderlines of each department involved
- ✓ Develops and prepares the customer acceptance policy, and submits it to the Board of Directors for consideration and approval.
- ✓ Prepares a risk management procedures manual in relation to preventing money laundering and terrorist financing.
- ✓ Monitors and evaluates the proper and effective implementation of the policy, practices, measures, procedures and controls put in place and in general the application of the risk management procedures manual.

- ✓ Receives information from the employees that creates a belief or suspicion of money laundering or terrorist financing or might be associated with such activities. The information is obtained in a written report form referred to as "Internal Money Laundering Suspicion Report" (attached as Appendix 1).
- ✓ Examines and evaluates the information received for any suspicious transactions, by referring to any other relevant information and discuss the circumstances of the case with the reporting employee and where appropriate with the management. The evaluation of the reported information will be made on a separate form which will be registered and retained on file. The form is referred as "Money Laundering Compliance Officer's Internal Evaluation Report" attached as Appendix 2.
- ✓ The compliance officer can decide to disclose the above information to the Unit for Combating Money Laundering. Sample of this report (hereinafter referred to as "Money Laundering Compliance Officer's Report to the Unit for Combating Money Laundering" attached to as "Appendix 3".
- ✓ However in case the Compliance and AMLO decides not to notify the Unit for Combating Money Laundering, then he/she explains the reason for such a decision on the "Money Laundering Compliance Officer's Internal Evaluation Report"
- ✓ Prepares and maintains a registry with the types of customers' categorization following a risk based approach. "Categorization of Customers on a Risk Basis" manual The Compliance and AMLO evaluates, at least on an annual basis, all risks arising from existing customers, new products and services and updates and amends systems and procedures applied by the Company for the effective management of the aforesaid risks.
- ✓ Evaluates the systems and procedures applied by a third person
- ✓ Ensures that the branches and subsidiaries of the Company operate in countries that taken all necessary measures for applying full compliance with the requirements of the Law, in relation to customer identification procedures, due diligence and record keeping procedures.
- ✓ Provides advice and guidance to the employees on the correct implementation of procedures and controls against money laundering and terrorist financing.
- ✓ Acquires the necessary knowledge and skills
- ✓ Makes recommendations and revise policies to screen transactions for customers or transactions the Company deems to be of significantly high risk (which may include persons, entities or countries that are contained on lists issued by government/international bodies) that special attention to such customers or transactions is necessary prior to completing any such transactions.
- ✓ The officer is responsible to provide advice and guidance to employees as appropriate on money laundering matters; determines whether the employees need further training; in direct consultation with the departmental manager as well as the BoD on any issues in relation to money laundering; is expected to avoid errors and/or omissions, especially with validating the reports received on money laundering activities. Organizes appropriate training sessions/seminars and prepares and applies an annual staff training program and evaluates the adequacy of the training given.
- ✓ The Officer maintains a registry with the Internal Money Laundering Suspicion Reports, the Money Laundering Compliance Officer's Internal

Evaluation Reports, Money Laundering Compliance Officer's Reports, also evaluation reports and any information in relation to the execution of his/her duties.

- ✓ The Officer obtains and utilizes, the county assessment reports on money laundering issued by the Financial Action Task Force, regional international bodies, Moneyval Committee and the International Monetary Fund and the World Bank.
- ✓ The Money Laundering officer is responsible for consulting with the company's senior management and internal audit department, as well as the Financial Services Authority, being the supervisory authority recognized by Law on money laundering matters.

Compliance Officer's Report

The Report of the AMLO is a significant tool for assessing the Company's level of compliance with its obligation laid down in the Law. The AMLO's Report shall be prepared and be submitted to the Board.

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

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

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

(c) the number of Internal Suspicion Reports submitted by Company personnel to the AMLO, and possible comments/observations thereon

(d) the number of reports submitted by the AMLO to the Unit, with information/details on the main reasons for suspicion and highlights of any particular trends

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

(f) summary figures, on an annualised basis, of Clients' total cash deposit in USD and other currencies in excess of the set limit of USD 10.000 (together with comparative figures for the previous year) as reported in the monthly prevention statement. Any comments on material changes observed compared with the previous year are also reported

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

(h) information on the systems and procedures applied by the Company for the ongoing monitoring of Client accounts and transactions

(i) information on the measures taken for the compliance of branches and subsidiaries of the Company, if any, due diligence and record keeping procedures and comments/information on the level of their compliance with the said requirements

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

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

(l) results of the assessment of the adequacy and effectiveness of staff training

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

(n) information on the structure and staffing of the department of the AMLO 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.

Stages of Money Laundering

The type of suspicious transactions that may be used for money laundering and terrorist financing is almost limitless. A suspicious transaction is often incompatible with the known and legitimate work of the client or his/her personal activities or with the normal turnover of the account, or otherwise with the financial profile that has been created by the company for the customer. The company certifies that always holds sufficient information and knowledge of the activities of its customers in order to be able to recognize early that a transaction or series of transactions are unusual or suspicious.

Examples of Suspicious transactions/activities

- ✓ Transactions without clear economic purpose or unnecessarily complex transaction.
- ✓ 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.
- ✓ Transactions or the size of transactions requested by the customer do not comply with his/her normal practice and business activities.
- ✓ Large volume of transactions and/or money deposited or credited into, an account when the nature of the customer's business activities would not appear to justify such activity.
- ✓ When the business relationship of the customer consists of only one transaction or lasts for a short period of time.
- ✓ There is no visible justification for a customer using the services of the company. For example a client whose address is located quite far from the company and in an area where he could be served by another Company.

- ✓ There are frequent transactions in the same financial instrument without obvious reason or under circumstances that appears unusual (Churning).
- ✓ There are frequent small purchases of a particular financial instrument by a customer who settles in cash, and then the total number of the financial instrument is sold in one transaction with settlement in cash or with the proceeds being transferred, with the customer's instructions, in an account other than his usual account.
- ✓ Any transaction the nature, volume or frequency appears to be unusual. For example the cancellation of an order, especially after the deposit of the consideration
- ✓ Transactions which are inconsistent with normal market practice, in relation to the size of the order and the frequency.
- ✓ The settlement of any transaction, especially large transactions in cash.
- ✓ Settlement of the transaction by a third person which is different than the customer which gave the order
- ✓ Instructions of payment to a third person which has no obvious link/connection with the instructor.
- ✓ Transfer of funds to and from countries or geographical areas which do not apply or they apply inadequately FATF's recommendations on money laundering and terrorist financing. Customer is unwilling to provide complete information when establishes a business relationship regarding the nature and purpose of its business, anticipated account activity, prior banking relationships, names of its officers and directors, or information on its business location. The customer usually gives little or misleading information that is difficult or costly for the company to verify.
- ✓ Client gives unusual or suspicious identification documents that their authenticity cannot be directly verified.
- ✓ Customer's home/business telephone is disconnected.
- ✓ Customer makes frequent or large transactions and has no record of past or present employment experience.
- ✓ Difficulties or delays on the submission of the financial statements or other identification documents, of a customer/legal person A customer who has been introduced by an overseas Financial Institution or 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.
- ✓ Shared address for individuals involved in cash transactions, especially when the address is also a business location and/or does not appear to correspond to the stated occupation (e.g. student, unemployed, self-employed, etc).
- ✓ The declared profession of the customer is not commensurate with the level or size of the executed transactions
- ✓ Financial transactions for non-profit or charitable organizations, for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- ✓ Unexplained inconsistencies arising during the customer identification (e.g. regarding previous or current county of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth etc).
- ✓ Complex trust or nominee network

- ✓ 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
- ✓ Use of general nominee documents in a way that restricts the control exercised by the company's Board of Directors.
- ✓ Changes in the lifestyle of employees, for example luxurious way of life or avoidance or absence from the office due to holidays.
- ✓ Changes in performance and behavior of employees

Terrorist Financing

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
- Narcotics trafficking

Legal fund raising methods used by terrorist groups include:

- Collection of membership dues and/or subscriptions
- Sale of books and other publications
- Cultural and social events
- Donations
- Community solicitations and fund raising appeals

Funds obtained from illegal sources are laundered in the following ways:

- Cash smuggling by couriers or bulk cash shipments
- Structured deposits to or withdrawals from bank accounts
- Purchases of monetary instruments – traveler's cheques, bank cheques, money orders
- Use of credit or debit cards
- Wire transfers by using straw men
- False identities
- Front and shell companies
- Nominees from among their close family members, friends and associates

Non-profit organizations

The use of a non-profit and charitable organization for raising funds and/or serving as cover for transferring funds in support of terrorists' acts can be made in the following ways:

- Establishing a non-profit organization with a stated charitable purpose but which actually exists only to channel funds to a terrorist organization
- 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
- A sudden increase in the frequency and amounts of financial transactions for the account of a nonprofit organisation.
- Large and unexplained cash transactions
- The absence of contributions from donors located within the country of origin of the non-profit organisation

There are four stages of money laundering during which there may be numerous transactions made by the launderers that could alert the Company to criminal activities:

- **Placement** - the physical disposal of cash proceeds derived from illegal activity;
- **Structuring** - a form of placement where the launderer makes many small cash deposits instead of a large one to evade local regulatory reporting requirements applicable to cash transactions;
- **Layering** -Refers to the creation of complex networks of transactions which attempt to obscure the link between the initial entry point and the end of the laundering cycle ;
- **Integration** - the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system, appearing to be normal business funds.

Application of Appropriate Measures and Procedures on a Risk Based Approach

The Company shall apply appropriate measures and procedures, by adopting a risk-based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be comparatively higher. The adopted risk-based approach that is followed by the Company, and described in the Manual, has the following general characteristics:

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

The risk-based approach adopted by the Company, and described in the Manual, involves specific measures and procedures in assessing the most cost effective and appropriate way to identify and manage the money laundering and terrorist financing risks faced by the Company. Such measures include:

- identifying and assessing the money laundering and terrorist financing risks emanating from particular Clients, financial instruments, services, and geographical areas of operation of its Clients

- managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls
- continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

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

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

The AMLO shall be responsible for the adequate 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 AMLO, at least annually.

Based on the above the MLCO proceeds in categorization of each Client into three categories:

- (a) High Risk
- (b) Normal Risk
- (c) Low Risk

The categorization of a Client affects the type and extent of measures the Company adopts, to manage and mitigate the identified risks cost effectively. These measures and procedures 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.

Identification of Risks

The risk-based approach adopted by the Company involves the identification, recording and evaluation of the risks that have to be managed. The Company shall assess and evaluate the risks it faces, for usage of the services provided for the purpose of money laundering or terrorist financing. The particular circumstances of the Company determine suitable procedures and measures that need to be applied to counter and manage risk.

In the cases where the services and the financial instruments that the Company provides are relatively simple, involving relatively few Clients or Clients with similar characteristics, then the Company shall apply procedures that focus on those Clients who fall outside the 'norm'. The Company shall be, at all times, in a position to demonstrate to SCB 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 and terrorist financing.

Company Risks

The following, *inter alia*, are sources of risks which the Company faces with respect to money laundering and terrorist financing:

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

- complexity of ownership structure of legal persons
- companies with bearer shares
- companies incorporated in offshore centres
- PEPs
- Clients engaged in transactions which involves significant amounts of cash
- Clients from high risk countries or countries known for high level of corruption or organised crime or drug trafficking
- unwillingness of Client to provide information on the Beneficial Owners of a legal person.

(b) *Risks based on the Client's behaviour:*

- Client transactions where there is no apparent legal financial/commercial rationale
- situations where the origin of wealth and/or source of funds cannot be easily verified
- unwillingness of Clients to provide information on the Beneficial Owners of a legal person.

(c) *Risks based on the Client's initial communication with the Company:*

- non face-to-face Clients
- Clients introduced by a third person.

(d) *Risks based on the Company's services and financial instruments:*

- services that allow payments to third persons/parties.
- large cash deposits or withdrawals
- products or transactions which may favour anonymity

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

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

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

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

Dynamic Risk Management

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Clients' activities change as well as the services and financial instruments provided by the Company change. The same happens to the financial instruments and the transactions used for money laundering or terrorist financing. In this respect, it is the duty of the AMLO to undertake regular reviews of the characteristics of existing Clients, new Clients, services and financial instruments and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics. These reviews shall be duly documented, as applicable, and form part of the Annual Money Laundering Report.

Relevant International Organisations

For the implementation of appropriate measures and procedures on a risk based approach, and for the implementation of Client Identification and Due Diligence

Procedures, the AMLO shall consult data, information and reports [e.g. Clients from countries which inadequately apply Financial Action Task Force's (hereinafter "FATF"), country assessment reports that are published in following relevant international organisations:

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

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

(c) The EU Common Foreign & Security Policy (CFSP)-
http://ec.europa.eu/external_relations/cfsp/sanctions/list/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.

Employees' Responsibilities

The Company expects each of its employees to conduct business in accordance with applicable anti money laundering laws, corporate policies, and the highest ethical standards. Employees will not in any way provide services or other assistance to clients who attempt to violate or avoid anti money laundering laws or corporate policies.

The employees will be held personally liable in case they fail to disclose information or suspicion of money laundering or terrorist financing. Employees are aware of their responsibilities and legal obligations; often and at least annually they attend education and training programs/seminars. The educational programs aims to update and inform them on any new developments in the field of preventing money laundering and terrorist financing, including, laws, regulations, trends and practical methods used for this purpose. The training is repeated at regular intervals to ensure that employees are reminded of their duties and obligations and are kept informed about any new developments.

The employees inform AMLO of any suspicious transactions or doubt without delay. The information is given in a form referred to as "Internal Suspicious Report" First Appendix.

The assessment of the information received by the employees is made on a form referred to as "Internal Evaluation Report" Second Appendix.

AMLO of the Company is responsible for approving or rejecting any suspicious transaction. His/her decision will be considered final and binding upon all employees. AMLO is responsible for carrying out monitoring of customers' accounts to detect suspicious activity, and if any found, reporting this internally to the Board of Directors, and carrying out necessary corrective actions, including further investigation of client and/or transaction, making an assessment, and may decide to report to the Unit.

In case the Compliance officer decides to disclose the information to Unit for Combating Money Laundering, prepares a written report to be submitted, referred to as "Compliance Officer's Report to the Unit for Combating Money Laundering" Third Appendix.

The Company's employees failing to adhere to this Procedure shall face internal disciplinary actions including termination of employment.

Education and Training

(a) The AMLO shall ensure that its employees are fully aware of their legal obligations according to the Law, by introducing a complete employees' education and training program

(b) the timing and content of the training provided to the employees of the various departments will be determined according to the needs of the Company. The frequency of the training can vary depending on to the amendments of legal and/or regulatory requirements, employees' duties as well as any other changes in the financial system of the Republic

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

(d) the training program will have a different structure for new employees, existing employees and for different departments of the Company according to the services that they provide. On-going training shall be given at regular intervals so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments.

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

AMLO Education and Training Program

The Senior Management of the Company shall be responsible for the AMLO of the Company to attend external training. Based on his/her training, the AMLO will then provide training to the employees of the Company. The main purpose of the AMLO training is to ensure that relevant employee(s) become aware of:

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

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

“Know Your Customer - KYC”

International and local laws oblige the Company as an international financial company carrying on relevant business activities, to establish and maintain appropriate “know your customer” procedures, which includes an understanding of your clients business, source of funds, as well as ensuring that the Company understands the investment objectives of its customers and is aware of their relevant investment experience. However, it is important that the Company’s customers conform to the Company’s principles and standards.

Prior to establishing a business relationship with a new customer, among other things, the following principles are considered as a part of the “know your customer” process:

- ✓ The Company will not accept as clients persons engaged in unethical behavior or in illegal activities;
- ✓ The Company will not accept as customers parties that cannot make a well informed and reasonable judgment as to the activities in which they are engaged;
- ✓ The Company will not accept as customers persons unwilling to provide sufficient documents/data and information as provided in the Customers acceptance policy

maintained by the Company The Company will accept only those new customers who complete appropriate account opening documentation with the Company.

The Company will initiate a relationship with a prospective or potential client only when it becomes fully satisfied that the Client complies with “know your customer” and due diligence procedures which includes:

- ✓ Verification of the customer’s identity on the basis of the documents provided by the customer as per the Customer’s acceptance Policy named as “Specific Customer Due Diligence and Identification Procedures”, (attached). Before conducting a business relationship with a new customer, his/her identity must be verified to ensure that a new relationship with the potential customer does not negatively affect the reputation of the Company.

Any transaction without prior establishment of the customer’s identity is prohibited according to the Company’s policies and procedures.

Training and awareness

A key component in managing the money laundering risk is to ensure that all employees, including senior management, fully understand the money laundering risks and their legal obligations and responsibilities. This is achieved through regular and focused training and awareness sessions. Training and awareness sessions are provided to all employees frequently and this includes all relevant employees including senior management.

Training is relevant to the anti-money laundering rules and policies and the content is adapted for various sectors of employees. It is also important to

mention that the Company keeps records of all training delivered and maintains a register of employee attendance.

New employees arrived in the Company receive AML training before undertaking their duties. Furthermore employees keeps notes from the seminars/courses and certificates of attendance.

Training can be delivered using a variety of different approaches. The company may offer private training to the employees or internal training conducted by the Compliance and Anti-Money Laundering Officer of the Company, or through seminars and courses designed by SCB or other institutions. The Company ensures that the training is relevant, up to date and tailored to an individual's needs. Effective and meaningful employee training is fundamental in managing the money laundering risk within the Company and it is essential that it is delivered in a manner that employees will find interesting and informative and also that it is conducted by persons who have the necessary expertise, knowledge and experience.

Training includes the following:

- How to recognize and handle transactions suspected to be associated with money laundering
- Awareness of office policies and procedures which are in place to prevent money laundering (e.g. client identification, internal reporting and record keeping)
- Updates as well as training on the relevant legislation relating to money laundering, and any new laws, regulations published by the Authority.

Monitoring

The electronic monitoring of transactions is an issue that is receiving a great deal of attention by the financial services industry. More and more transactions are being undertaken electronically, without any human intervention, providing those involved in money laundering with greater opportunities to launder money and to remain undetected.

There is recognition by the industry and regulators that the electronic monitoring of transactions can provide some protection in dealing with this risk. A monitoring system can provide an effective way of identifying potential money laundering transactions.

Transactions executed for the client are compared and evaluated against the anticipated movement of the account, the standard turnover, business and customer data/information held and according to the economic profile of the customer. Significant deviations are investigated and the findings recorded in the file of the client.

Transactions which cannot be explained by the information available for the customer, receive further examination to determine whether any suspicions of money laundering or terrorist financing appears. The Compliance Officer evaluates and examines the information received (Internal Suspicion Report) by reference to other relevant information and discusses the circumstances of the case with the informer and where appropriate with the management of the

Company. The evaluation of the information is registered on a report referred to as Internal Evaluation Report.

The Company's Anti-Money Laundering Procedures

The following Policy has been derived from the general principles, laws, and regulations for combating Money Laundering as developed by the SCB, Financial Action Task Force and the Basel Committee for Organization Supervision.

The Company has in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the organization from being used, intentionally or unintentionally, by criminal elements. The Company has in place adequate Know your Customer (KYC) programs. Such essential elements start from the services, risk management and control procedures and include:

- customer acceptance policy,
- customer identification,
- on-going monitoring of high risk accounts
- Risk management.
- Categorization of clients on a risk basis

The Company is obliged not only to establish the identity of its customers, but also to monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC constitutes a core feature of services' risk management and control procedures. The intensity of KYC programs beyond these essential elements is tailored to the degree of risk.

1. Customer acceptance policy

The Company maintains clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to an organisation. Before accepting a potential client, KYC and due diligence procedures are followed, by examining factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators.

Quite extensive due diligence is essential for an individual with a high net worth whose source of funds is unclear. No cash is accepted as means of trading when accepting a new client. All new clients' money is transferred through a reputable bank. Banks have their own anti-money laundering procedures. A decision to enter into business relationships with higher risk customers, such as politically exposed persons is taken exclusively at senior management level.

2. Customer identification

Customer identification is an essential element of KYC standards. For the purposes of this paper, a customer includes:

- ✓ The person or entity that maintains an account with the company or those on whose behalf an account is maintained (i.e. beneficial owners);
- ✓ The beneficiaries of transactions conducted by professional intermediaries;

- ✓ Any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the company.

The Company maintains a systematic procedure for identifying new customers and cannot enter into a service relationship until the identity of a new customer is satisfactorily verified.

Procedures “document and enforce policies for identification of customers and those acting on their behalf”. The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit. The Company pays special attention in the case of non-resident customers and in no case, short-circuit identity procedure is followed just because the new customer is unable to present enough documents and information to satisfy the KYC and due diligence procedures followed.

The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, the Company undertakes regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if the Compliance and Anti-Money Laundering Officer becomes aware at any time, through compliance and/or AMLO reviews, that it lacks sufficient information about an existing customer, takes immediate steps to ensure that all relevant information is obtained as quickly as possible.

The Company can be exposed to reputational risk, and should therefore apply enhanced due diligence to such operations. Private accounts, which by nature involve a large measure of confidentiality, can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalized investment company. In each case reputational risk may arise if the company does not diligently follow established KYC procedures. All new clients and new accounts are approved by at least one person, the managing director or the compliance officer. In case of a new high risk customer, the final decision is taken by the managing director. Particular safeguards have been put in place internally to protect confidentiality of customers and their business, the Company ensures that equivalent scrutiny and monitoring of these customers and their business is conducted, e.g. it is available to be reviewed by compliance officer and auditors.

Company maintains clear standards and policies, on what records must be kept on customer identification and individual transactions and their retention period”. Such a practice is essential to permit the company to monitor its relationship with the customer, to understand the customer’s on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to criminal prosecution.

As the starting point and natural follow-up of the identification process, the company obtains customer identification papers and retain copies of them for at least five years after an account is closed. The company also retains all financial transaction records for at least five years from the date when a firm’s relationship with the client was terminated or a transaction was completed.

General identification requirements

The Company obtains all information necessary to establish to its full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account.

When an account has been opened, but problems of verification arise in the service relationship, which cannot be resolved, the company can close the account and return the money to the source from which they were received. While the transfer of an opening balance from an account in the customer's name in another organisation subject to the same KYC standard, it will be considered, however we will do our own KYC procedures because we should nevertheless consider the possibility that the previous account manager may have asked for the account to be removed because of a concern about dubious activities.

Naturally, customers have the right to move their business from one organization to another. However, if the company has any reason to believe that an applicant is being refused service facilities by another organisation, applies enhanced due diligence procedures to the customer.

The company will never agree to open an account or conduct ongoing business with a customer who insists on anonymity or who gives a fictitious name. Nor should confidential numbered accounts function as anonymous accounts but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff. Whereas a numbered account can offer additional protection for the identity of the account-holder, the identity must be known to a sufficient number of staff to operate proper due diligence.

Customer Identification Process

Specific Customer Due Diligence and Identity Procedures (attached)

Client identification must be carried out as soon as reasonably practicable after first contact is made. Except its obligation to exercise due diligence and customer identification, the Company must confirm that the identity info which holds for its customers has to remain fully informed and updated with all necessary identification and information throughout their business relationship. The Company review and monitor on a regular basis the validity and adequacy of customer identification information in its possession.

Notwithstanding the above and taking into account the degree of risk, if realized at any time during the business relationship that the Company lacks sufficient or reliable evidence (data) and information on the identity and financial profile of an existing customer, the Company immediately takes all necessary actions using the identification procedures and measures to provide due diligence, in order to collect the missing data and information as quickly as possible and in order to determine the identity and create a comprehensive financial profile of the customer.

Furthermore the Company monitors the adequacy of the information held and identity and economic portrait of its customers when and where one of the following events occurrences:

Conduct of a significant transaction that appears to be unusual and/or significant than the usual type of trade and economic profile of the client;

A significant change in the situation and legal status of the client as:

- change of directors/secretary
- Change of registered shareholders and/or actual beneficiaries,
- Change of registered office,
- Change of trustees
- Change of corporate name and/or trade name,
- Change of main trading partners and/or significant new business;

A significant change on the way and operating rules of the client's account, such as:

- Change of persons authorized to handle its account,
- Request for opening a new account in order to provide new investment services and/or financial instruments

In case of customer transaction via internet, phone, fax or other electronic means where the customer is not present to verify the authenticity of his/her signature, or that is the person who actually owns the account, or is authorized to handle the account, the Company established reliable methods, procedures and practices to control access to electronic means to ensure that deals with the actual owner or authorized signatory of the account.

Where the client refuses or fails to provide the Company with the required documents and information for identification and creation of economic portrait, before entering into the business relationship, or during the execution of an individual transaction without adequate justification the Company will not proceed in a contractual relationship or will not execute the transaction and may also report it to the Unit. This can lead to a suspicion that the client is engaged in money laundering and terrorist financing.

If during the business relationship the client refuses or fails to submit all required documents and information, within reasonable time, the Company has the right to terminate the business relationship and close the accounts of the client. The compliance officer also examines weather to report the case to the Unit.

Resident Personal Customers details required

1. True name and/or names used
2. Current permanent address, including postal code
3. Date of birth
4. Profession or occupation

Names should be verified by reference obtained from a reputable source which bears a photograph, such as:

- current valid full passport
- national id card

In addition to the clients' name verification, the current permanent address should be verified by (originals) by obtaining any one of the following:

- Copy of a recent utility bill
- Local tax authority bill
- Bank statement
- Checking a telephone directory

In an addition to the above an introduction from a respected customer personally known to the Manager of the Company or from a trusted member of staff, can assist the verification procedure. Details of the introduction should be recorded on the customer's file.

Non-Resident Personal Customer

The verification procedure is similar to that for residents, and the same information should be obtained.

In addition:

- ✓ Where client contact is face-to-face;
- ✓ The address verification may be difficult, but can still use passports or identity cards, with photos.
- ✓ If in doubt seek to verify identity with a reputable credit or financial institution in the customers country of residence

Where client contact is non face-to-face;

- ✓ Verification of identity and current address should be sought from a reputable credit or financial institution in the applicant's country of residence.

Accounts for Corporate Customers:

- ✓ Company searches, and other commercial enquiries, to ensure that the applicant has not been or in the process of being dissolved, struck off, wound up or terminated.
- ✓ Changes to company structure occur or ownership occur subsequently, further checks should be made.
- ✓ Identity verification should aim to identify
 - The company
 - The directors
 - All persons duly authorized to operate the account
 - In case of private companies, the major beneficial shareholders
 - The company's business profile in terms of nature and scale of activities

The following Documents are required:

- ✓ The original or certified copy of the Certificate of incorporation
- ✓ Memorandum and articles of association
- ✓ Resolution of the Board of Directors to enter into transactions on the stock market and conferring authority to those who will act for the customer
- ✓ Where appropriate a search of the file at the Companies' Registry
- ✓ Identity of individuals who are connected with the company

Creation of an economic portrait

- ✓ The Company must be satisfied that is dealing with a real person, and for this purpose, obtains sufficient identification documents to prove that is the person who claims to be.
- ✓ The Company must verify the identity of beneficial owners of accounts. For legal persons, receives such data and information to understand the ownership and control structure of the customer. Regardless of the customer's type (e.g. natural or legal person, partnership or sole trader), we take adequate data and information on the customer's business activities and the expected pattern and level of transactions.
- ✓ The identity of all customers is verified on the basis of reliable data and information given or received from independent and reliable sources, i.e. those data and information that is difficult to be falsified or to be obtained in an illegal way.
- ✓ The home address and work is considered a key element of the identity of a person
- ✓ In no case is accepted as evidence the same info (data), for identifying a customer's identity and residence proof.

All data and information must be collected before entering into the business relationship in order to create the financial portrait of the client and, as a minimum, includes the following:

- ✓ the purpose and justification (reason) for the conclusion of the business relationship;
- ✓ the anticipated turnover of the account, the nature of transactions, the expected source of money to be credited to the account and the expected destination of outgoing payments;
- ✓ the size of assets and annual income, a clear description of the major business / professional activities / work.

The data and information that makes the financial portrait of the client - legal person include:

- company name,
- Country of incorporation,
- headquarters address,
- names and identity of beneficial owners,
- directors, authorized signatories,
- financial data,
- information for the group that may be owned by the company (Country of incorporation of mother company, subsidiaries and associated companies, the principal activities, financial results).

All above data and information will be recorded on a separate form which is filed in the client's file along with all other documents, and internal memos from the minutes of the meetings with the client. This form is updated in regular intervals or whenever new information on any changes or additions occurs to the elements that makes the financial profile of the customer.

Simplified Customer due diligence and identification procedures

The Company may apply simplified customer due diligence and identification procedures, provided that the Company collects sufficient information to establish if the customer qualifies for an exemption.

Simplified procedure is applied to the following customers:

- ✓ Credit or financial institutions.
- ✓ Credit or financial institution carrying out one or more of the financial business activities as defined in section the law, which:
 - in accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing, 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 which is subject to disclosure requirements consistent with community legislation;
- ✓ Domestic public authorities should comply with the following requirements:
 - the identity is publicly available, transparent and certain;
 - The customers activities, as well as its accounting practices are transparent;
 - They are subject to a community institutional organ or the authorities of a member state, or they are subject to adequate procedures ensuring the control of their activity

Enhanced due diligence measures

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

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

- i. obtain additional documents, data or information for verifying the Client's identity
- ii. take supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution
- iii. ensure that the first payment of the operations is carried out through an account opened in the Client's name with a credit institution.

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

- i. gather sufficient information about the credit institution-Client to understand fully the nature of the business and the activities of the Client and to assess, from publicly available information, the reputation of the institution and the quality of its supervision
- ii. assess the systems and procedures applied by the credit institution-Client for the prevention of money laundering and terrorist financing
- iii. obtain approval from the Senior Management before entering into correspondent bank account relationship
- iv. document the respective responsibilities of the person engaged in financial or other business activities and of the credit institution-Client

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

(c) In respect of transactions or Business Relationships with PEPs, the Company shall:

- i. have appropriate risk-based procedures to determine whether the Client is a PEP
- ii. have Senior Management approval for establishing Business Relationships with such Clients
- iii. take adequate measures to establish the source of wealth and source of funds that are involved in the Business Relationship or transaction
- iv. conduct enhanced ongoing monitoring of the Business Relationship.

Enhanced customer due diligence measures is taken in all other instances which due to their nature entail a higher risk of money laundering or terrorist financing.

Reliance on third parties for Client Identification and Due Diligence

1. The Company may rely on third parties for the implementation of Client identification and due diligence procedures, provided that:
 - (a) the third person makes immediately available all data and information, which must be certified true copies of the originals, that were collected in the course of applying Client identification and due diligence procedures
 - (b) the Company applies the appropriate due diligence measures on the third person with respect to his professional registration and procedures and measures applied from the third person for the prevention of money laundering and terrorist financing, according to the provisions of the Law.
2. Third party means credit institutions or financial institutions or auditors or independent legal professionals, falling under the Law and which:
 - (a) they are subject to mandatory professional registration, recognised by law; and
 - (b) they subject to supervision regarding their compliance with the requirements of the Law.
3. Further to point 2 above, third party may also be any other person who is engaged in financial business, or accountants or independent legal professionals and which according to a relevant decision of the Advisory Authority, have been determined that they impose equivalent procedures and

measures for the prevention of money laundering and terrorist financing to those laid down by the Law.

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

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

5. Further to point 3 above, in the case where the third person of subparagraph (1) is an accountant or an independent legal professional or a trust and company services provider from a country that the Advisory Authority has determined to be applying procedures and measures for the prevention of money laundering and terrorist financing equivalent to the Law, then the Company, before accepting the Client identification data verified by the said third person, shall apply the following additional measures/procedures:
 - (a) the AMLO or the appointed person shall assess and evaluate the systems and procedures applied by the third person for the prevention of money laundering and terrorist financing, as applicable
 - (b) as a result of the assessment of point (a) above, the AMLO must be satisfied that the third person implements Client identification and due diligence systems and procedures which are in line with the requirements of the Law
 - (c) the AMLO shall maintain a separate file for every third person of the present paragraph, where it stores the assessment report of point (a) and other relevant information (for example identification details, records of meetings, evidence of the data and information of point 2 above)
 - (d) the commencement of the cooperation with the third party and the acceptance of Client identification data verified by the third person is subject to approval by the AMLO

The AMLO shall be responsible for the implementation of the provisions mentioned in this Section of the Manual. The Internal Auditor shall be responsible to review the adequate implementation of the provisions mentioned herein, at least annually.

On-going monitoring and Recording of accounts and transactions

On-going monitoring is an essential aspect of effective KYC procedures. The constant monitoring of the Clients' accounts and transactions is an imperative element in the effective controlling of the risk of money laundering and terrorist financing.

The Company can only effectively control and reduce the risk if it has an understanding of normal and reasonable account activity of its customers so that it has means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, it is likely to fail in its duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so. The extent of the monitoring needs to be risk-sensitive.

For all accounts, the Company has systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention is paid to transactions that exceed these limits.

In this respect, the AMLO 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.

Certain types of transactions alert to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense (big transactions), or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer.

Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account.

There is intensified monitoring for higher risk accounts. The Company has set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors.

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

(a) the identification of:

- transactions which, as of their nature, may be associated with money laundering or terrorist financing
- unusual or suspicious transactions that are inconsistent with the economic profile of the Client for the purposes of further investigation.
- in case of any unusual or suspicious transactions, the head of the department providing the relevant investment and/or ancillary service as well as the Head of the Administration/Back Office Department, as applicable, shall be responsible to communicate with the AMLO

- (b) further to point (a) above, the investigation of unusual or suspicious transactions by the AMLO. The results of the investigations are recorded in a separate memo and kept in the file of the Clients concerned
- (c) the ascertainment of the source and origin of the funds credited to accounts
- (d) the use of appropriate IT systems.

For higher risk accounts:

The company ensures that it has adequate management information systems (this review is performed by our risk management committee on a regular basis, the information and the market pals are received through different informative sources in Russia such as press release, economic release etc.) to provide managers and compliance officer with timely information needed to identify, analyze and effectively monitor higher risk customer accounts. The types of reports that may be needed include reports of missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the organization.

Senior management in charge of business knows the personal circumstances of the organization's high-risk customers and is alert to any sources of third party information. Significant transactions by these customers are approved by a senior manager.

Company developed a clear policy and internal guidelines, procedures and controls and remains especially vigilant regarding business relationships with PEPs and high profile individuals or with persons and companies that are clearly related to or associated with them. As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, regular reviews are undertaken.

Reporting of Suspicious Transactions to the Unit

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 AMLO its suspicion to the Unit.

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

In order to identify suspicious transactions the AMLO shall perform the following activities:

- monitor on a continuous basis any changes in the Client's financial status, business activities, type of transactions etc
- monitor on a continuous basis if any Client is engaged in any of the practices described in the list containing examples of what might constitute suspicious transactions/activities related to money laundering and terrorist financing
- receive and investigate the information from Company's employees, on suspicious transactions which creates the belief or suspicion of money laundering. This information is reported on the Internal Suspicion Report. The said reports are archived by the AMLO
- evaluate and check the information received from the employees of the Company, with reference to other available sources of information and the exchanging of information in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained on the report which is submitted to the AMLO is evaluated on the Internal Evaluation Report, which is also filed in a relevant file
- if, as a result of the evaluation described above, the AMLO decides to disclose this information to the Unit, then he prepares a written report, which he submits to the Unit
- if as a result of the evaluation described above, the AMLO decides not to disclose the relevant information to the Unit, then he fully explain the reasons for his decision on the Internal Evaluation Report.

Submission of information to the Unit

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

- (a) the identity of the account holders
- (b) the identity of the Beneficial Owners of the account
- (c) the identity of the persons authorised to manage the account
- (d) data of the volume of funds or level of transactions flowing through the account
- (e) connected accounts
- (f) in relation to specific transactions:
 - the origin of the funds
 - the type and amount of the currency involved in the transaction

- the form in which the funds were placed or withdrawn, for example cash, cheques, wire transfers
- the identity of the person that gave the order for the transaction
- the destination of the funds
- the form of instructions and authorisation that have been given
- the type and identifying number of any account involved in the transaction

Record Keeping

Under the Law the Company is required to keep records for a period of at least five years. The five year period is calculated following the carrying out of the transactions or the end of the business relationship.

According to Section 68 (1) of the Law the following records must be kept:

- ✓ Copies of the evidential material of the customer identity.
- ✓ Relevant evidential material and details of all business relations and transactions, including documents for recording transactions in the accounting books and
- ✓ Relevant documents of correspondence with the customers and other persons with whom they keep a business relation.

All documents and information are available rapidly and without delay to the Unit and the competent Supervisory Authorities for the purpose of discharging the duties imposed on them by the Law. The Unit needs to be able to compile a satisfactory audit trail. Document retention may be in original documents or certified true copies and be kept in hard copy, or other format such as electronic form given that they can be available at any time and without delay.

When setting up document retention policies, the Company considers the statutory requirements and the potential needs of the unit. Documents and information must be original or true copies. In cases where the documents are being certified by another person and not the Company, or the third party, then the documents must be apostilled or notarized.

Format of Records

The Administration/Back Office Department shall retain the documents/data mentioned above, other than the original documents or their Certified true copies that are kept in a hard copy form, in other forms, such as electronic form, provided that the Administration/Back Office Department shall be able to retrieve the relevant documents/data without undue delay and present them at any time, to SCB or to the Unit, after a relevant request. In case the Company will establish a documents/data retention policy, the AMLO shall ensure that the said policy shall take into consideration the requirements of the Law. The Internal Auditor shall review the adherence of the Company to the above, at least annually.

Certification and language of documents

The documents/data obtained, shall be in their original form or in a certified true copy form. In the case that the documents/data are certified as true by a different person than the Company itself or by the third person, the documents/data must be apostilled or notarised.

A true translation shall be attached in the case that the documents above are in a language other than English.

Each time the Company shall proceed with the acceptance of a new Client, the AMLO shall be responsible for ensuring compliance with the provisions of the above.

Risk management

Effective KYC procedures embrace routines for proper management oversight, systems and controls, segregation of duties, training and other related policies. The board of directors of the Company is fully committed to an effective KYC program and procedures and ensures their effectiveness. Explicit responsibility is allocated within the organization for ensuring that the company's policies and procedures are managed effectively and are in accordance with local supervisory practice. The channels for reporting suspicious transactions are clearly specified and communicated to all personnel.

Under anti-money laundering rules, each month we provide statements of large cash transactions to the supervisory authority Financial Services Authority.

Services' internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence of KYC policies and procedures. As a general rule, the compliance function provides an independent evaluation of the organization's own policies and procedures, including legal and regulatory requirements. Its responsibilities include ongoing monitoring of staff performance through sample testing of compliance and review of exception reports to alert senior management or the Board of Directors if it believes management is failing to address KYC procedures in a responsible manner.

Internal audit plays an important role in independently evaluating the risk management and controls, discharging its responsibility to the Audit Committee of the Board of Directors through periodic evaluations of the effectiveness of compliance with KYC policies and procedures, including related staff training. Management ensures that audit functions are staffed adequately with individuals who are well versed in such policies and procedures. In addition, internal auditors are proactive in following-up their findings and criticisms.

The company maintains an ongoing employee-training program so that the staff is adequately trained in KYC procedures. The timing and content of training for various sectors of staff is adapted by the company for its own needs. Training requirements should have a different focus for new staff, front-line staff, compliance staff or staff dealing with new customers. New staff should be educated in the importance of KYC policies and the basic requirements at the organisation. Staff members who deal directly with the customers are trained to verify the identity of new customers, to exercise due diligence in handling accounts of existing customers on an ongoing basis and to detect patterns of suspicious activity. Regular refresher training is provided to ensure that

employees are reminded of their responsibilities and are kept informed of new developments. It is crucial that all relevant staff fully understand the need for and implement KYC policies consistently. A culture within services that promotes such understanding is the key to a successful implementation.

SPECIFIC CUSTOMER DUE DILIGENCE AND IDENTITY PROCEDURES

A. Natural persons Resident:

1. True name and / or names used, based on the official identity card or passport
 - i. Document issued by an independent and reliable source and which bears a photograph of the customer
2. Full permanent address in the Republic, including the postcode
 - i. Visit the customer's home
 - ii. Presentation of a recent (up to 6 months) telephone bill, electricity, municipal taxes, or bank account statement, or similar, with the above, documents (to protect against the presentation of forged or counterfeit documents, the presentation of original documents is required).
3. Phone number, landline and mobile, and fax
4. e-mail address, if any
5. Date and place of birth
6. Nationality
7. Details of profession and other occupations, including the name of the employer / business organization
8. In addition to the above, where the client was introduced by a trusted member of the staff of the Company, or by other reliable existing client or a third person personally known, member of the Board of Directors, details of these recommendations must be produced and kept in the client's file.

B. Natural persons Non-Resident

1. True name and / or names used, based on the official identity card or passport
 - i. Document issued by an independent and reliable source and which bears a photograph of the customer
 - ii. data obtained must disclose the number, date and country of issuance of passport and date of birth of the client
2. Full permanent address, including the postcode
 - i. presentation of a recent (up to 6 months) telephone bill, electricity, municipal taxes, or bank account statement, or similar, with the above, document (for protection against the presentation of false documents, the presentation of original documents is required).
3. Phone number, landline and mobile, and fax
4. e-mail address, if applicable
5. Date and place of birth
6. Nationality
7. Details of professional and other occupations, including the name of the employer / company
8. In addition to the above, where the client was introduced by a trusted member of the staff of the Company, or by other reliable existing client or a third person personally known, member of the Board of Directors, details of these recommendations must be produced and kept in the client's file.

9. Information regarding public places (functions) owned or held by the customer during the last twelve months and whether is a close relative or close associate of such person in order to determine whether the customer is a politically exposed person

- i. "politically exposed persons" means the natural persons who have been entrusted with prominent public functions and their immediate family members or persons known to be close associates of such persons.

C. Joint accounts

In cases of joint accounts, of two or more persons, the identity of all persons (individuals) that hold or have the right to manage the account, must be verified, as set out in Part A and B above where appropriate.

D. Accounts of unions, societies, clubs, provident funds and charitable institutions

1. memorandum and articles of association
2. registration documents
3. certificate of registration
4. list of the members of the Board of Directors/ management Committee
5. the identity of all authorized persons
6. follow identification procedures for the above persons as defined in Part A and B above

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

1. Identity of the directors/partners (Part A and B)
2. identity of the beneficiaries (Part A and B)
3. Identity of authorized persons (Part A and B)
4. In the case of partnerships, the original or a certified true copy of the partnership's registration certificate
5. business address
6. nature and size of its activities
7. the financial portrait of the legal person
 - ✓ identity info
 - ✓ identity of beneficiaries
 - ✓ in case of legal persons (ownership and control structure, of the customer)
 - ✓ information regarding the business activities and the expected pattern and level of transactions
 - ✓ residence and business address
 - ✓ the purpose and reason for the establishment of a business relationship
 - ✓ anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited to the account and the expected destination of outgoing transfers/payments
 - ✓ the customer's size of wealth and annual income, and a clear description of the main business / professional activities / operation
 - ✓ company's name, Country of incorporation, head offices address, names and identity of beneficial owners, directors, authorized signatories, financial information, ownership structure of the group that the company may be a part of (Country of incorporation of the parent company, subsidiaries and associate companies, the main activities, financial information)

8. Where a formal partnership agreement exist, must be provided and also a mandate from the partnership authorizing the opening of the account and confirming authority to a specific person who will be responsible for its operation.

F. Accounts for Legal Persons

1. Registration number – certificate of registration
2. Registered name and trade name used
3. Full corporate registered address and head officers
4. Phone number, fax and email address
5. Members of the Board of Directors
6. Persons authorized to operate the account and to act on behalf of the legal person
7. Real beneficiaries of private and public companies that are not listed in regulated market with equivalent disclosure and transparency requirements.
8. Registered shareholders that act as nominees of the actual beneficiaries'
9. the financial portrait of the legal person identity info
 - ✓ identity of beneficiaries
 - ✓ in case of legal persons (ownership and control structure, of the customer)
 - ✓ information regarding the business activities and the expected pattern and level of transactions
 - ✓ residence and business address
 - ✓ the purpose and reason for the establishment of a business relationship
 - ✓ anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited to the account and the expected destination of outgoing transfers/payments
 - ✓ the customer's size of wealth and annual income, and a clear description of the main business / professional activities / operation
 - ✓ company's name, Country of incorporation, head offices address, names and identity of beneficial owners, directors, authorized signatories, financial information, ownership structure of the group that the company may be a part of (Country of incorporation of the parent company, subsidiaries and associate companies, the main activities, financial information)
10. certificate of incorporation
11. good standing certificate
12. certificate of registered address
13. Certificate of directors and secretary
14. memorandum and articles of association
15. certificate of registered shareholders in the case of private and public companies that are not listed in regulated market in a country with equivalent disclosure and transparency requirements
16. a resolution of the board of directors for opening the account and granting authority to those who will operate it
17. In case of nominee shareholders of the actual beneficiaries, a copy of the trust deed signed between the nominee shareholder and the beneficial owner, by virtue of which the registration of the shares on the name of the nominee shareholder on behalf for the real Beneficiary has been agreed
18. Documents and data to establish, the identity of persons authorized by the legal person to operate the account, as well as the registered shareholders and beneficial owners of the legal person
19. Where necessary, a copy of the latest audited financial statements (if available) and / or copies of its latest management accounts.

20. It is noted that at any times during the business relationship, the Company can obtain additional documents and information if required.

As an additional measure the Company can conduct research and receive information from the records of the Registrar of Companies and Official Receiver of the Republic (for Cypriot companies) in order to ensure that the company (legal person) is not nor is in the process of being dissolved or liquidated or struck off the registry and that it continues to be registered as an operating company.

G. Accounts for Legal Person (Companies or Legal Entities) outside the Republic

1. All documents and information as stated in Part F above must be provided
2. The Company can conduct research and receive information from the Companies Registry or equivalent authority in the country of incorporation (legal entity) abroad (for non-Cypriot companies) and / or request information from other sources in order to ensure that the company (legal person) is not nor is in the process of being dissolved or liquidated or struck off the registry and that it continues to be registered as an operating company.

Shareholder – another entity

In case of client - legal person applying for the conclusion of a business relationship or the execution of an occasional transaction and whose sole or direct shareholder is another legal person, before proceeding to the following must be provided:

1. all documents as provided in Part F
2. ownership structure
3. identity of the individual beneficial owners or/and control the other legal person
4. Identity of persons who have the ultimate control over the legal person's business and assets as describes in Part A & B
5. In the cases that the ultimate control is in the hands of the persons who have the power to manage the funds, accounts or investments of the legal person, without the need for further authorization and who would be in a position to override the internal procedures, we need the identity of persons exercising effective control, as defined in Part A & B, even if they have no direct or indirect interest or an interest of less than 10% of ordinary share capital or voting rights of the legal person.

SHAREHOLDER-TRUST

If the beneficial owner of an entity is a trust then the following documents are required:

1. Name
2. Date of establishment
3. Identity of the trustor (Part A & B)
4. Identity of the trustee (Part A & B)
5. Identity of the beneficial owners (Part A & B)
6. The nature and purpose of the establishment and activities (memorandum and articles of association)
7. origin of the money, extracts from the trust agreement is needed and other relevant information from the trustees

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

1. A license or authorization from a competent supervisory/regulatory authority of the country of incorporation and operation to provide the said services
2. Evidence that are subject to the supervision for the prevention of money laundering and terrorist financing purposes.
3. In case the person is incorporated and/or operating in a third country the following must be obtained:
 - i. all documents as stated above in Part H
 - ii. copy of the license or authorization granted from a competent supervisory/regulatory authority of its country of incorporation and operation
 - iii. Sufficient data and information to fully understand the control structure and management of the business activities and the nature of the services and activities provided by the customer.
4. In the case of investment funds and mutual funds the Financial Organisation must provide the following:
 - i. Identity of the beneficial owners
 - ii. Information regarding their objectives and control structure, including documentation and information for the verification of investment managers, investment advisors, administrators and custodians

I. Nominees or agents of third persons

The following information is required:

1. Verify the identity of the nominees or the agent of the third person (Part A & B)
2. Verify the identity of any third person on whose behalf the nominee is acting (Part A&B)
3. Copy of the authorization agreement that has been concluded between the interested Parties

NOTE: THE COMPANY AT ANY TIME CAN INQUIRE AND OBTAIN ADDITIONAL DOCUMENTS AND INFORMATION IF REQUIRED IF AT ANY LATER STAGE ANY CHANGES OCCUR IN THE STRUCTURE OF THE OWNERSHIP STATUS OR TO ANY DETAILS, THE CUSTOMERS HAS TO INFORM THE COMPANY AND PROVIDE ANY NEW INFORMATION AND DOCUMENTS.

IF IN THE COUNTRY OF THE POTENTIAL/EXISTING CLIENT ANY OF THE REQUIRED DOCUMENT DOES NOT EXIST IN THE FORM REQUIRED BY THE COMPANY THE COMPLIANCE OFFICER MAY ACCEPT A SIMILAR DOCUMENT SERVING THE NEEDS OF DUE DILIGENCE.

FIRST APPENDIX

**INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND
TERRORIST FINANCING**

INFORMER'S DETAILS

Name:
Tel:
Department:
Fax:
Position:

CUSTOMER'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 Unit: Yes/No ... Date Reported:
Ref.....

SECOND APPENDIX

**INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND
TERRORIST FINANCING**

Reference:
Customer's Details:
Informer:
Department:

INQUIRIES UNDERTAKEN (Brief Description)

.....
.....

ATTACHED DOCUMENTS

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

COMPLIANCE OFFICER'S DECISION

.....
.....

FILE

NUMBER.....

COMPLIANCE OFFICER'S SIGNATURE DATE

.....

THIRD APPENDIX

COMPLIANCE OFFICER'S REPORT TO THE UNIT FOR COMBATING MONEY LAUNDERING

I. GENERAL INFORMATION

Financial Organization's Name: _____

Address where customer's account is kept:

Date when a business relationship established or occasional transaction was carried out:

Type of account(s) and number(s): _____

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

(A) NATURAL PERSONS

	<u>Account Beneficiary(ies)</u>	<u>Authorised Signatory(ies)</u>
Name(s):	_____	_____
	—	
	_____	_____
	—	
Home address(es):	_____	_____
	—	
	_____	_____
	—	
	_____	_____
	—	
	_____	_____
	—	

Job Address(es):

—	
—	
—	

Profession / Employer's Details :

—	
—	
—	

Place and Date of birth:

—	
—	
—	

Nationality and passport number:

—	
—	
—	

(B) LEGAL ENTITIES

Company name, country: _____
and date of incorporation _____

Office Address: _____

Main Operations: _____

	<u>Name</u>	Nationality and passport number	Date of Birth	<u>Home address</u>	<u>Profession and employer's details</u>
<u>Registered Shareholder(s)</u>	1. _____ 2. _____ 3. _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
<u>Beneficial owner(s)</u> (if other than those mentioned above)	1. _____ 2. _____ 3. _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
<u>Directors/ Managers</u>	1. _____ 2. _____ 3. _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____
<u>Authorised Signatories</u>	1. _____ 2. _____ 3. _____	_____ _____ _____	_____ _____ _____	_____ _____ _____	_____ _____ _____

III. SUSPICIOUS TRANSACTION DETAILS

Please provide detailed information about the suspicious transaction:

1.

2.

3

(4) ASSERTION / SUSPICION OF MONEY LAUNDERING

(please explain the factors leading to the assertion / suspicion of money laundering)

IV OTHER INFORMATION

- Other services offered to the client(s)

Compliance Officer's Signature

Date

.....

.....

Notice:

The report should be accompanied with photocopies of the following:

1. Natural persons: Those pages of the passport that prove the client's identity.
2. Legal entities: Certificate of Incorporation/registration of the company/partnership , directors and shareholders.
3. All the documents associated with the suspicious transaction(s)