Anti-Money Laundering Manual

Limassol, October 2019

CONTENTS

01 GENERAL PROVISIONS

NBH Markets EU Limited (hereinafter also called the «Company») is a legal entity duly registered in the Republic of Cyprus with No. 291974; it is a private company limited by shares within the meaning of Companies Law Cap. 113, as amended, and is a Cyprus Investment Firm (or «CIF») with License No. 208/13 and governed by all applicable EU and local Regulations including European Markets in Financial Instruments Directive II («MiFID II») AND the Cyprus Investment Services and Activities and Regulated Markets of 2017 («Law 87(I)/2017»), as amended.

The Company is supervised and regulated by the Cyprus Securities and Exchange Commission (hereinafter also called «CYSEC» or the «Commission» or the «Regulator») in accordance with the provisions of the law, Directives and Circulars issued by the Commission and legislation governing the roles and responsibilities of the Regulator.

As a person carrying on financial activities, the Company must comply with the provisions of the Applicable Legislation. For the purposes of this Manual the term «Applicable Legislation» shall include The Prevention and Suppression of Money Laundering and Terror Financing (Amending) Law 13(I) of 2018, as amended (hereinafter also called «The Law Combating Money Laundering (hereinafter called «MOKAS») following the transposition and implementation of Directive (EU) 2015/849 ("AMLD IV"); Amending Law 158(I) of 2018; Directive DI144-2007-08 regarding the Prevention of Money Laundering and Terrorist Financing as amended issued by the Commission (hereinafter called «AML Directive»), DIRECTIVE (EU) 2018/843 (“AMLD V”) amending Directive (EU) 2015/849 (“AMLD IV”) of the European Parliament and the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (hereinafter called «EU Directive»); ESAs Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on anti-money laundering and countering the financing of terrorism – 'The Risk Factors Guidelines', Directives, Circulars, Reporting Forms and other documents of the Commission which address the issues related to the Anti-Money Laundering procedures and any other legislative act of the European Parliament, MOKAS and the Commission currently in force substituting or amending the above mentioned. Definitions and terms stated in the text of this Manual shall have same meanings as those stated in the Law, applicable Directives, Circulars, Regulations and other documents of European Council, MOKAS and the Commission.

The Purpose of this Anti-Money Laundering Internal Operation Manual (hereinafter also called «The Manual») is to determine and to describe the procedures, policies, regulations and mechanisms which are established, implemented and maintained by the Company in compliance with the Applicable Legislation. The 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. For this Manual, the term ‘money laundering’ will include terrorist financing unless otherwise stated.

Strict compliance with the provisions of this Manual is obligatory for each officer, employee, Director and other relevant persons of the Company. The Manual is notified to all of the Company’s personnel.

Failure to comply with the provisions of this Manual may result in civil, disciplinary or criminal sanctions against the Company and/or its Employees, as well as damage the Company’s reputation.

This document is designed strictly for internal use of the Company and its relevant persons; the Manual or any part of its contents could be disclosed and/ or made available to other persons, including Auditors and Supervisory Authorities only in cases and on the conditions, which are prescribed by this Manual and Applicable Legislation.

In addition to the provisions of this Manual, duties and responsibilities of Money Laundering Compliance Officer and Designated Board Member, contents of Annual Report of AMLCO, Client Identification and Due Diligence procedures are described in the Internal Operation Manual of the Company.

02 ANTI-MONEY LAUNDERING POLICY AND PROCEDURES

Money Laundering is the process of disguising the illegal sources and ownership of proceeds derived from criminal activities. The criminals may attempt to use the financial organizations in order to conceal and to control the illegitimate proceeds and to use such monetary funds by integrating them with funds derived from legitimate sources without discovery or interruption of the criminal activities.

The Company acknowledges that combating the financial crime and money laundering is one of its most important tasks and recognizes the importance of the fact that any failure in detection and/ or prevention of such attempts with high probability might entail the financial and reputation damages, regulatory and legal sanctions (legal risk, reputation risk, concentration risk and operational risk).

The Company has developed and implemented the policy which ensures the prevention of use of the Company for the legalization of proceeds of criminal activities and for financing of terrorism (hereinafter covered by the term «Money Laundering»). Such policy determines that AML activities are performed as ongoing process using risk-based approach. It should be regularly reviewed and, if necessary, improved basing on the latest regulatory requirements and best practices applied in the industry.

The objective of this policy is to protect the Company's reputation, eliminate the possible vulnerability and to prevent the imposition of sanctions against it as a result of any actions and/ or omissions which may lead to the use of the Company, intentionally or unintentionally, for legalization of illegitimate proceeds, through conduct of the business/customer relationship with the Company.

This policy is implemented through specific procedures, established following the requirements of Applicable Legislation and includes the utilization of relevant information systems for monitoring of transactions and development of Know Your Client («KYC») policy.

Anti-Money Laundering procedures assume the involvement of all the Officers, Employees and Departments of the Company assuming the clear assignment of roles and responsibilities; the most important roles in development, implementation and assessment of these procedures are performed by the Board of Directors, the Designated Board Member (described in Section 3 of the Manual) and the Money Laundering Compliance Officer (described in Section 4 of the Manual).

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. KYC policy used by the Company is aimed at prevention of Money Laundering and limitation of inherent risks, its main components are Client Acceptance Policy, Client Identification procedures, monitoring of transactions and accounts and risk management.

All the data regarding the identity and transactions of the Client (Client Agreements, copies of correspondence with a Client, supporting documents for transactions, authorization documents, photocopies of documents on the basis of which the certification of Client identity was made and other relevant documents) shall be kept by the Company for the period of least five years since the termination of the Company's relationship with this Client and/ or since the carrying out of the transactions on his behalf.

Retention of documents other than in the original printed form or certified true copies may be kept in other ways, such as electronic form, provided that the Company is able to retrieve the relevant documents and data without undue delay and present them at any time, to the Commission or to MOKAS, after a request. The documents/ data submitted by the Clients are presented in their original form or in a certified true copy form. A true translation form is attached in the case that the documents/ data are executed in a language other than English.

03 RESPONSIBILITIES OF THE BOARD OF DIRECTORS AND DESIGNATED BOARD MEMBER, OTHER EMPLOYEES

The role and responsibility of the board of directors and the designated board member of the Company in relation to the prevention of money laundering and terrorist financing is particularly important.

Duties and responsibilities of the Board of Directors and Designated Board Member of the Company in relation to the prevention of money laundering are the following:

- Determination, record and approval of the general policy principles of the Company in relation to the prevention of money laundering and terrorist financing and communication of them to the Money Laundering Compliance Officer («AMLCO»),
- Ensuring that all requirements of Applicable Legislation are applied, and assuring that appropriate, effective and sufficient systems and controls are introduced for achieving this requirement on a continuous basis,
- Approval of the present Manual, its communication to all employees of the Company that manage, monitor or control in any way the clients' transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined,
- Appointment of Money Laundering Compliance Officer and determination of his/ her their duties and responsibilities,
- Assuring that the Money Laundering Compliance Officer and his/her assistants 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,

- Ensuring that all employees are aware of the person who has been assigned the duties of the Money Laundering Compliance Officer to whom they shall report any information concerning transactions and activities for which they have knowledge or suspicion that might be related to money laundering and terrorist financing,
- Establishment of a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the Money Laundering Compliance Officer and applicable notification of AMLCO for its explicit prescription in the present Manual,
- Ensuring that the Money Laundering Compliance Officer has sufficient resources, including competent staff and technological equipment, for the effective discharge of his/ her duties,
- Assessment and approval of the Annual Report of AMLCO and taking all actions as deemed appropriate under the circumstances to remedy any weaknesses and/ or deficiencies identified in this Report.
- Ensuring that the Company maintains at all time a Designated Board Member, who shall be responsible for the implementation of this Manual and other polices or procedures in relation with the 'Applicable Legislation" and "The Law" and of the directives and/or circulars and/or regulations issued pursuant thereto including any relevant acts of the European Union.

Performing its duties, the BoD also assess and approve recommendations made by Internal Audit Function assuring that appropriate, effective and sufficient systems and controls related to AML are introduced and functioning properly on a continuous basis.

Obligations of the Internal Audit Function:

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.

Following the report, responsibilities of the Board of Directors of the Company are:

- To meet and decide the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected in the Internal Auditor's report. The minutes of the said decision of the Board and the Internal Auditor's report shall be submitted to CySEC within twenty days of the said meeting, and not later than three months from the end of the calendar year.

Duties and responsibilities of AMLCO are described in Section 4 of this Manual.

Employees of the Company may be personally liable for failure to report information or suspicion, regarding money laundering or terrorist financing.

All the Company's employees shall cooperate and report, without delay, anything that comes to their attention in relation to transactions for which there is a slight suspicion that they are or might be related to money laundering or terrorist financing.

It is understood that the employees fulfil their legal obligation to report their suspicions regarding money laundering and terrorist financing, after meeting the above requirement. The Company's employees failing to adhere to this Manual shall face internal disciplinary actions including termination of employment.

Obligations of the AML Director

In accordance with the AML Directive, the Company has assigned one member of the Board to be designated as the responsible person for the implementation of the legal framework related to the prevention and suppression of money laundering and terrorist financing («AML Director»). The designated member of the Board may be either executive or non-executive and will ensure the Company's compliance with all provisions of the present Law and of the directives and/or circulars and/or regulations issued pursuant thereto including any relevant acts of the European Union.

The AML Director is required to keep in regular and systematic contact with the Money Laundering Compliance Officer and the Alternate Money Laundering Officer in order to ensure that there is frequent collaboration between the Board and the Money Laundering Compliance Officer Department. The AML Director oversees the duties and responsibilities of the Money Laundering Compliance officer, as these are detailed in the AML Manual of the Company.

The AML Director further ensures that the staff receives an appropriate level of AML/CFT training relevant to the role they undertake within the regulated entity, with particular attention in the area of suspicious activity monitoring and reporting and establishing whether the training received allows the staff to effectively fulfil its responsibilities.

Education and Training

a. The AMLCO shall ensure that its employees are fully aware of their legal obligations according to the Law and the Directive, by introducing a complete 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.

AMLCO Education and Training Program:

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

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

04 ANTI MONEY LAUNDERING COMPLIANCE OFFICER

An Officer is appointed by the Board of Directors as Money Laundering Compliance Officer («AMLCO») of the Company in order to command the necessary authority. Such person should have sufficient qualification and given necessary authority to coordinate all AML activities on the Company's level and communicate directly with the BoD.

As soon as the CySEC issues a relevant announcement with the certification of AMLCOs' or any persons who perform at any degree the duties of the AMLCO, the Company shall proceed with the required actions in order to ensure its compliance with the relevant legislative requirements.

Duties and responsibilities of Money Laundering Compliance Officer include, but are not limited to the following:

- Design, based on the general policy principles, of the internal practice, measures, procedures and controls relevant to the prevention of money laundering and terrorist financing, describes and allocate the limits of responsibility of each department. It is provided that, the above include measures and procedures for the prevention of the abuse of new technologies and systems providing financial services, for the purpose of money laundering and terrorist financing, as well as measures so that the risk of money laundering and terrorist financing is appropriately considered and managed in the course of daily activities of the Company with regard to the development of new products and possible changes in the Company's economic profile (penetration into new markets),
- Development and establishment of the Clients Acceptance Policy, which is described in Section 5 of this Manual and submits it to the Board of Directors for consideration and approval,
- Monitoring and assessment of the correct and effective implementation of the policy, practices, measures, procedures and controls relevant to the prevention of money laundering and terrorist financing, and, in general, the implementation of the provisions in the present Manual. In this regard, AMLCO is obliged to apply appropriate monitoring mechanisms which will provide him all the necessary information for assessing the level of compliance of the Departments and employees of the Company with the procedures and controls which are in force. In the event that AMLCO identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, he/she shall give appropriate guidance for corrective measures and where deems necessary shall inform the Board of Directors,
- AMLCO suggests and personally implements risk based controlling mechanisms of the Client's trading and non-trading operations and keep proper records,
- Analysis of risks of money laundering of new services, Financial Instruments and new types of products and transactions, which the Company may be engaged in on own behalf or on behalf of its Clients, provision of relevant advice to the concerned Departments and to the Board of Directors of the Company,

- Receiving from the Company's employees the information, which is considered to be the knowledge, or suspicion of money laundering activities, or might be related to such activities. The information is received in a written report form («Internal Suspicion Report», Annex II of this Manual),
- Evaluation and examination of the information received from the employees, by reference to other relevant information and discussion of circumstances of the case with the informer and, where appropriate, with the Management of the Company. The evaluation of this information is being done on an «Internal Evaluation Report» (Annex III of this Manual),
- If following the evaluation Money Laundering Compliance Officer decides to notify MOKAS, then he/she completes a written report and submits it to MOKAS the soonest possible,
    - Currently used system for reporting to MOKAS (goAML) implies that AMLCO is registered as a reporting person in this electronic system and is obliged to comply with the procedures as stated in the relevant legislation of the Commission.
    - It is provided that, after the submission of the AMLCO's report to MOKAS, the accounts involved and any other connected accounts, are closely monitored by the Money Laundering Compliance Officer and following any directions from MOKAS, he/ she must thoroughly investigate and examine all the transactions of the accounts.
- If following the evaluation AMLCO decides not to notify MOKAS, then he/ she fully explains the reasons for such a decision in the «Internal Evaluation Report»,
- Acting as the first point of contact with MOKAS, upon commencement and during an investigation as a result of filing a report to MOKAS,
- Ensuring the preparation and maintenance of the lists of clients categorised following a risk-based approach, which contains, at least, the names of clients, their account identifications and the dates of the commencement of the business relationship. Additionally, AMLCO ensures the updating of the said lists with all new or existing clients, in the light of additional information obtained,
- Detection, recording and evaluation, at least on an annual basis, all risks arising from existing and new clients, new Financial Instruments and services and updates and amends the systems and procedures applied by the Company for the effective management of the relevant risks,
- Provision of advice and guidance to the employees of the Company on subjects related to money laundering and terrorist financing,
- Acquiring of the required level of knowledge and skills for the improvement of the procedures appropriate for recognising, preventing and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing,
- Determination of the Company's Departments and Employees that need further training and education for the purpose of prevention of money laundering and terrorist financing, and organisation of appropriate training sessions/ seminars. In this regard, AMLCO shall prepare and apply an annual staff training program and to assess the adequacy of the education and training provided,
- Preparation and timely submission to the Commission of the Monthly Prevention Statement and provision of the necessary explanation to the appropriate employees of the Company for its completion,
- On a monthly basis, submission to the Commission of the Form 144-08-11 which includes details for the total cash deposits accepted by the Company (or any other applicable form implemented by the Commission), the Internal Suspicions Reports, and the Money Laundering Compliance Officer's Reports to MOKAS. The completion of the Form provides the opportunity to the Company initially to evaluate and, subsequently, to reinforce its systems of control and monitoring of its operations, for the purpose of early identification and detection of transactions in cash which may be unusual and/or carry enhanced risk of being involved in money laundering and terrorist financing operations. This Form is completed and submitted to the Commission within 15 (fifteen) days from the end of each month,
- Response to all requests and queries from MOKAS and the Commission, provision of all requested information and full cooperation with MOKAS and the Commission,
- Maintenance of a registry which includes the Internal Suspicion Reports and Internal Evaluation Reports and relevant statistical information (Department that submitted the internal report, date of submission to AMLCO, date of assessment, date of reporting to MOKAS), the evaluation reports and all the documents that verify the accomplishment of his duties applicable to circulation, submission, receipt and storing of these reports,
- During the execution of his/ her duties and the control of the compliance of the Company with the requirements of Applicable Legislation, AMLCO must obtain and utilise data, information and reports issued by relevant international organizations,
- Preparation of the Annual Report in accordance with the provisions of Circular C033 regarding the content of the Annual AMLCO Report.

Annual Report, prepared by the Money Laundering Compliance Officer is submitted for approval to the Board of Directors, within two months from the end of each calendar year (i.e. by the end of February at the latest) and, upon its approval by the Board of Directors, within 20 days is submitted to the Commission. It is provided that during the approval of this Report, the

Board of Directors identify and implement the measures decided for the correction of any weaknesses and/ or deficiencies identified in the Report and establish implementation timeframe.
Annual Report dealing with money laundering and terrorist financing preventive issues relevant to the year under review covers, at least, the following issues:

0. Executive Summary

Executive summary summarises the lengthy text of the Report and includes the following:

- Introduction
- Purpose/ objectives/ terms of reference
- Key findings/weaknesses (a summary of all key findings/weaknesses, regardless of whether they have been rectified, or not, within the year, and the key issues from previous years that are still pending).
- Suggestions
- Conclusion

The Executive Summary will be included in the beginning of the Annual Report.

1. Regulatory Framework and Information from Relevant International Organizations

- Reference to changes or upcoming changes (if already known) of the regulatory framework regarding the prevention of money laundering and terrorist financing, such as:
  - In the Prevention and Suppression of Money Laundering Activities Laws of 2007-2018, as in force ("the Law").
  - In the relevant Commission's Directives.
  - In the relevant Commission's Circulars.
- Reference to relevant data, information, reports from international organizations (FATF, Moneyval, IMF, Council of the European Union, UN, etc.) taken into consideration in the measures and procedures applied by the Company for the prevention of money laundering and terrorist financing.
- Specific measures and procedures taken/adopted concerning the paragraphs above.
- Suggestions for further measures and implementation of further procedures in the case of any weaknesses or deficiencies in relation to paragraphs above, setting a timeframe for implementation

2. Inspections and Reviews by the AMLCO

- Analytical reference to inspections and reviews performed by the AMLCO to determine the degree of compliance of the Company in the policy, practices, measures, procedures and controls applied for the prevention of money laundering and terrorist financing. Specific reference to the content and the method/way of conduct of the inspections and reviews, regarding, at least, the following sectors:
  - Completeness of the risk management and procedures manual regarding money laundering and terrorist financing.
  - Implementation of customers' acceptance policy.
  - Construction and content of economic profile.
  - Identification of suspicious transactions, internal suspicion reporting and external reporting to MOKAS.
  - Simplified customer identification and due diligence procedures of low risk customers.
  - Customer identification and due diligence measures of normal risk customers.
  - Enhanced customer identification and due diligence procedures of high-risk customers.
  - Timing of customers' identification.
  - Reliance on third parties for customer identification and due diligence purposes.
  - Ongoing monitoring of customers' accounts and transactions.
  - Record keeping.
  - Implementation of measures and procedures on a risk-based approach.
  - Implementation of the financial sanctions imposed by the United Nations and the European Union.
  - Measures and procedures taken for the compliance of branches and subsidiaries of the Company, operating in countries outside the European Economic Area, where applicable.
  - Education and training of staff.
- Specific results of the inspections and reviews of points above, indicating the significant deficiencies and weaknesses identified in the policy, practices, measures, procedures and controls applied by the Company for the prevention of money laundering and terrorist financing. In this regard, the seriousness of the deficiencies or weaknesses is noted, the risk implications, actions taken, and the recommendations made for rectifying the situation, setting a timeframe for implementation.

3. Internal Reporting

- Number of Internal Suspicion Reports submitted by the employees of the Company to the AMLCO and comparative data with the previous year.
- Number of Internal Suspicion Reports that have not been notified to MOKAS and comparative data with the previous year.
- Circumstances that led to the increase/decrease of Internal Suspicion Reports and significant trends observed.

4. External Reporting

- Information on cases related to money laundering and terrorist financing for which no report was made.
- Number of AMLCO's Reports to MOKAS, comparative data with the previous year, summary of data/information for the main reasons of the suspicion and significant trends observed.
- Feedback from MOKAS regarding the submitted Reports.

5. Customers' Cash Deposits

- Reference on an annual basis of customers' total cash deposits, in Euro and other currencies in excess of the set limit of 10.000 Euro (as reported in the Monthly Prevention Statement) and comparative data with the previous year.
- Circumstances that led to the increase of customers' cash deposits and significant trends observed.
- Reference in the measures and actions of the Company regarding cash deposits by customers (method/ way of identification and investigation, recording the investigation in the customer's file, result of the investigation and possible actions taken).
- Recommendations for further actions and implementation of further procedures in case of deficiencies and weaknesses in relation to paragraph above, setting a timeframe for implementation.

➢ *The company does not accept cash as a form of payment.*

6. High Risk Customers

- Information on the policy, measures, practices, procedures and controls applied by the Company in relation to high-risk customers (specific enhanced due diligence measures and details of ongoing monitoring of accounts and transactions for PEPs).
- Number, country of origin and type of high-risk customers with whom a business relationship was established, or an occasional transaction has been executed and comparative data with the previous year.

7. Ongoing Monitoring of Customers' Accounts and Transactions

- Taking into consideration the requirements of applicable legislation, adequate reference to information for the systems and procedures applied by the Company for the ongoing monitoring of customers' accounts (update of the economic profile and customer identification data) and the ongoing monitoring of customers transactions (including the source of funds) that are compared with the data and information that are kept in their economic profile. Among others, reference to the following:
  - Analysis of the way/method (automated or non-automated) of the ongoing monitoring of customers' accounts and transactions.
  - Details for any variation of the ongoing monitoring of customers' accounts and transactions according to the customer's categorization on a risk-based approach.
  - Details of the timing the ongoing monitoring of customers transactions (in real time or after the completion of an event).
  - Details of the way/method of documenting the ongoing monitoring of customers transactions (preparation of a memo describing all relative actions and recording it in the customer's file).
- Results the ongoing monitoring of customers' accounts and transactions during the year (several suspicious transactions identification, update several customers' accounts, internal report or report to MOKAS).

8. Branches and Subsidiaries Outside the European Economic Area (E.E.A) *(when applicable)*

- Data/information of the branches and subsidiaries of the Company that operated outside the European Economic Area (E.E.A).
- Taking into consideration the requirements of applicable legislation, measures and procedures taken for the compliance of branches and subsidiaries of the Company that operate outside the E.E.A.

9. Communication, Education and Training of Staff

- Reference to specific issues/cases, questions/clarifications and any other form of communication with the staff and the specific results that have arisen from the relevant communication.
- Taking into consideration the provisions of applicable legislation, information on training courses/seminars attended by the AMLCO and the rest of the staff of the Company during the year:
  - Summarized data of the program/ content of the training courses/seminars.
  - Number and duration of the training courses/ seminars.
  - Number and position of the employees participating in the training courses/ seminars.

- Number and position of employees who did not participate in the training courses/seminars and their duties are relevant with the prevention of money laundering and terrorist financing. Information on the reasons for not participating.
- Instructors' names and qualifications.
- Whether the training courses/ seminars were performed in-house or by an external organization or consultants.
- Information for the educational material received.

- Information on the specific way/ method with which the adequacy and effectiveness of staff training has been assessed and reference to the results.
- Taking into consideration the provisions of applicable legislation and the results of assessment stated in paragraph above, information on the training program which is recommended to attend for the AMLCO and the rest of the staff of the Company, for next year:
  - Summarized data of the program/content of the training courses/ seminars.
  - Number and duration of the training courses/seminars.
  - Number and position of the employees who will participate in the training courses/seminars.
  - Number and position of employees who will not participate in the training courses/ seminars and their duties are relevant with the prevention of money laundering and terrorist financing. Information on the reasons for not participating.
  - Instructors' names and qualifications.
  - Whether the training courses/seminars will be performed in-house or by an external organization or consultants.

10. Money Laundering Compliance Officer

- Name, location and date of employment of the AMLCO and data/ information in case the operation of AMLCO have been outsourced to a third party.
- Position / hierarchy and reporting lines of the AMLCO within the organizational structure of the Company including organizational chart.
- Duties of the AMLCO.
- Areas/ cases where AMLCO did not have complete and timely access to all information, data and documents that would assist him in the performance of his duties.
- Recommendations and implementation timeframe, for any additional staff and technical resources to reinforce the measures and procedures for the prevention of money laundering and terrorist financing.

05 CLIENT ACCEPTANCE POLICY

Client Acceptance Policy implemented by the Company is based on the requirements of Applicable Legislation. The main purpose of the Client Acceptance Policy is to protect the Company's good reputation continuously and consistently, and to prevent the Company from being used for fraudulent or criminal purposes. The underlying principle of the Client Acceptance Policy is that the Company should "know its customers" (Know-your-Client process / "KYC"). The Company's reputation can be harmed either by failing to act in accordance with regulators' principles or by dealing with counterparties whose business activities raises suspicions and/or who have bad reputation of their own. It does not mean that hush conclusions should be made on the bases of rumors and speculations. It aims at not allowing the commencement of business relationship or performance of one-off transactions with the Clients facing the charges for criminal activities, against whom any legally established sanctions are applied and who may attempt to use the Company for participation in criminal activities.

The ultimate responsibility for KYC obligations, both during the process of adoption and thereafter throughout the life cycle of the relationship, rests with the AML Compliance function. The AML Compliance function is responsible for monitoring developments in the field, identifying required action and informing and training all relevant personnel. The AML Compliance function is also responsible for the general over-viewing of the application of the prescribed procedures and the improvement / amendment of these procedures if the need arises.

The Company has established an on-line step-by-step procedure that needs to be followed by the potential Clients in order to submit an application to the Company for the establishment of a business relationship with the Company. Through the various steps of this procedure the Company ensures that it gathers the necessary KYC and customer due diligence documentation and information as required by the Law. All steps to be followed by the potential Clients are compulsory and all steps need to be completed by the potential Clients for a Client account opening application to be successfully submitted to the Company.

Each existing and prospective Client of the Company is assessed on a risk-based approach and the following criteria are considered:

- Country of domicile or residence of the Client

- Delivery channel risk factors (Face-to-face versus non-face-to-face Client; Intermediaries or introducers the firm might use)
- Background of the Client
- Professional or business activities of the Client
- Reputation of the Client
- Nature and behaviour of the Client
- Business objects of the Client
- The purpose of a business relationship (an account) of the Client
- Estimated annual turnover of the Client
- Origin of funds
- Transactions, services and products for which the Client applies
- Legal form/structure (in case of legal entities)
- Participation in lists of persons against whom the sanctions are imposed following the decisions of competent authorities of European Union, OFAC or other international organizations

The following categories of Clients are prohibited to enter into any type of business relationships with the Company:

- Clients who do not provide sufficient documents and/ or information for establishment and verification of their identity, their ownership structure and beneficial owners
- Clients who fall under sanctions based on decisions of competent authorities of European Union, OFAC or other international organizations
- Citizens of some countries where activity of the Company is prohibited

Foreign Account Tax Compliance Act (FATCA)

Without limiting the foregoing, the Company, a regulated Cyprus Investment Firm, is required to comply based on the Intergovernmental Agreement between Cyprus and the United States and has taken all reasonable steps to be considered in compliance with FATCA. The Client acknowledges and accepts that the Company, as a Foreign Financial Institution («FFI»), is required to disclose information in relation to any US reportable persons to the relevant authorities, as per the reporting requirements of FATCA https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca.

*The definition of U.S. reportable persons:

- A U.S. citizen (including dual citizen)
- A U.S. resident alien for tax purposes
- A domestic partnership
- A domestic corporation
- Any estate other than a foreign estate
- Any trust if: a court within the United States is able to exercise primary supervision over the administration of the trust, and
- One or more United States persons have the authority to control all substantial decisions of the trust
- Any other person that is not a foreign person.

Substantial U.S. ownership (U.S. person owns more than 10% of the shares of a corporation {vote or value} or of a partnership or of a trust) is also required to comply with FATCA.

"Lower Value Accounts"- Individual accounts with a balance or value as of June 30th, 2014 that exceeds $50.000, but does not exceed $1,000.000.

For accounts with a balance of value as of June 30th, 2014, that is below the threshold stated above there is no need for review, identification and reporting.

"High Value Accounts" – Individual accounts with a balance or value that exceeds $1,000.000 as of June 30th, 2014 or any subsequent year.

For accounts with a balance or value as of June 30th, 2014, that is below the threshold stated above but becomes a High Value Account as of the last day of a subsequent calendar year, the Company completes the enhanced review procedures with respect to such account within six months after the last day of the calendar year in which the account becomes a High Value Account.

In respect to the mentioned requirements, the Company has designed the process regarding the U.S. reportable persons in a very clear and simple way for its new and existing Clients.

For the Existing Clients:

The Company has created a pop-up window with a special questionnaire/declaration related to FATCA once the customer

logins to his or her "client area" for depositing and withdrawals, and as well for the trading purposes.

- In case the Client ticks YES, the system will allow such a Client to login in the usual manner.
- In case the Client ticks NO, i.e. the Client is not in agreement with the declaration/questionnaire, he or she is considered a U.S. Reportable Person. The Company is obliged to report specific information to the United States Internal Revenue Service (U.S. IRS) in relation to U.S. Reportable Persons.

The following pop-up window appears:

Dear Client, according to the information provided, you are considered as a U.S. Reportable Person. Without limiting the foregoing, the Company, a regulated Cyprus Investment Firm, is required to comply based on the Intergovernmental agreement between Cyprus and the United States. By acknowledging this notice, you are accepting and confirming that the Company, as an FFI (Foreign Financial Institution), is required to disclose information in relation to any U.S. Reportable Persons to the relevant authorities on an annual basis as per the reporting requirements of FATCA https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca.

Please provide with a following required documents for the reporting purpose:

- Name (stated on U.S. Passport)
- Address (in the U.S.)
- U.S. Passport copy, and
- U.S. Tax Identification Number (TIN)

The system will NOT allow to login to the "client area" for financial services without the provision of the above-mentioned documents.

For the New Clients:

The Company has amended a current registration page with the following details:

- In case the Client ticks NO, the following pop-up window appears:

FATCA COMPLIANCE QUESTIONNAIRE/DECLARATION FOR NATURAL PERSONS
U.S. Indicia
I am NOT a U.S. citizen or resident
My place of birth is NOT in the U.S.
I do NOT have a current U.S. mailing or residence address (including a U.S. post office box or U.S. "in-care-of" address)
I do NOT have a current U.S. telephone number
I do NOT have standing instructions to transfer funds to an account maintained in the United States
I do NOT have currently effective power of attorney or signatory authority granted to a person with a U.S. address
I do NOT have an "in-care-of" or "hold mail" address that is the sole address for the Account Holder? In the case of a Preexisting Individual Account that is a Lower Value Account, an "in-care-of" address outside the United States is not to be treated as U.S. indicia.
I do NOT have a U.S. Tax Identification Number

"I agree that to the best of my knowledge the information provided above is accurate and complete and no information has been withheld. "
Here, the Client have the option to accept (by clicking on YES or NO) electronically the above-mentioned declaration/questionnaire.

- In case the Client ticks YES, the system will allow such Client to continue the registration in the usual manner. With respect to new Individual Accounts, upon account opening, the Company collects all necessary documentation pursuant to AML/KYC Procedures.
- In case the Client ticks NO, i.e. the Client is not in agreement with the above declaration/questionnaire, he or she is considered a U.S. Reportable Person. The Company is obliged to report specific information to the United States Internal Revenue Service (U.S. IRS) in relation to U.S. Reportable Persons.

The following pop-up window appears:

Dear Client, according to the information provided, you are considered as a U.S. Reportable Person. Without limiting the foregoing, the Company, a regulated Cyprus Investment Firm, is required to comply based on the Intergovernmental agreement between Cyprus and the United States. By acknowledging this notice, you are accepting and confirming that the Company, as an FFI (Foreign Financial Institution), is required to disclose information in relation to any U.S. Reportable Persons to the relevant authorities on an annual basis as per the reporting requirements of FATCA https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca.

Please provide with a following required documents for the reporting purpose:

- Name (stated on U.S. Passport)
- Address (in the U.S.)
- U.S. Passport copy, and
- U.S. Tax Identification Number (TIN)

By providing necessary above-mentioned documents the Client continues the registration process in the usual manner.

For the new Entity Accounts:
The Company identifies the Controlling Persons as determined under AML/KYC procedures and resolves whether any such person falls under definition of U.S. Reportable Person.
If the Entity Account Holder falls under definition of U.S. Reportable Persons, the Company treats the account as a U.S. Reportable Account*.

Aggregation of Individual Accounts:
For purposes of determining the aggregate balance or value of financial accounts held by an individual, the Company aggregates all accounts maintained by the Company, to the extent that the Company's computerized system links the accounts by reference to a data element such as Client number or taxpayer identification number and allow account balances to be aggregated.

Aggregation of Entity Accounts:
For purposes of determining the aggregate balance or value of financial accounts held by an Entity, the Company takes into account all accounts held by Entities that are maintained by the Company, to the extent that the Company's computerized system links the accounts by reference to a data element such as Client number or taxpayer identification number and allow account balances to be aggregated.

Special Aggregation Rule Applicable to Relationship Manager:
For purposes of determining the aggregate balance or value of Financial Accounts held by a person to determine whether an account is a High Value Account, the Company requires, in the case of any accounts that a relationship manager knows or has reason to know are directly or indirectly owned, controlled, or established (other than in a fiduciary capacity) by the same person, to aggregate all such accounts.

Currency Transaction Rule:
For purposes of determining the balance or value of Financial Accounts denominated in a currency other than the U.S. dollar, the Company converts the dollar threshold amounts described into such currency using a published spot rate determined as of the last day of the calendar year preceding the year in which the Company is determining the balance or value.

Ongoing Monitoring of Compliance with FATCA Requirements:
In its Terms and Conditions of Business the Company refers to the reporting requirements of FATCA. Furthermore, the Company has implemented additional procedures for the ongoing monitoring of compliance with FATCA requirements to its CRM system. The Company reviews on an annual basis whether there is a change in the U.S. indicia of its clientele which might result in identifying U.S. Reportable Persons, the classification and reporting of the account as lower or high.

Ongoing Monitoring and Measures in Case of Change Clients Status on U.S. Reportable:
In order to be sure that existing Clients do not become U.S. Reportable Persons, the employees of the Back Office (on-boarding) Department will request updated questionnaire (i.e. the questionnaire/declaration provided by the Clients upon account opening) once per year. If the existing Account Holder falls under definition of U.S. Reportable Persons, the Company treats the account as a U.S. Reportable Account*.
The Company shall monitor the balance of any U.S. Reportable Person identified at the end of each calendar year. Relevant information on the account is reported to the Cyprus Tax Department on an annual basis.
The Company has been duly registered with the US IRS Authorities as deemed compliant with FATCA and other applicable laws and regulations in force and obtained its Global Intermediary Identification Number (GIIN) – JYQF8W.99999.SL.196.

Common Reporting Standard Regime (CRS)

The Common Reporting Standard ("CRS") refers to the common requirements and standards created by the Organization for Economic Cooperation and Development (OECD) for the automatic exchange of certain financial information between countries. The CRS Decree imposes obligations on Cyprus Financial Institutions to identify, maintain and report information about individuals and entities tax resident in another jurisdiction for whom they maintain financial accounts and to report in to the Cyprus Tax Department to the extent that it is reportable under the applicable legislation. An up to date list of the countries that have either signed or committed to adopt CRS can be found on the OECD's site at: http://www.oecd.org/tax/transparency/AEOI-commitments.pdf.

The Company is required to identify reportable accounts based on the information collected (via a self-certification) and report them accordingly to the local tax authority. In turn, the local tax authority will exchange information with the tax authorities of Reportable Jurisdictions.

Self-Certification means a certification by the Account Holder that provides the Account Holder's status and any other information that may be reasonably requested by the Reporting Cyprus Financial Institution to fulfil its reporting and due diligence obligations, such as whether the Account Holder is resident for tax purposes in a Reportable Jurisdiction.

The Company may not rely on a self-certification or documentary evidence if the Company knows or has reason to know that the self-certification or documentary evidence is incorrect or unreliable.

The Company is requested to report the account balance or value as of the end of the calendar year or if the account was closed during the year, the closure of the account. The Information to be reported is to be reported annually.

The information to the reported for CRS purposes, consists of the following:

- Name
- Address
- Tax Identification Number (TIN)
- Date and Place of Birth (for individuals only)
- The Account Number
- The account balance or value as at 31/12 or, if the account was closed during such year or period, the closure of the account.

Under new regulations all potential and existing Clients must provide information concerning the potential Client's tax residency for the Company to fulfil its reporting and due diligence obligations, such as whether the Account Holder is resident for tax purposes in a Reportable Jurisdiction. The Company may not rely on a self-certification or documentary evidence if the Company knows or has reason to know that the self-certification or documentary evidence is incorrect or unreliable. The Company is requested to report the account balance or value as of the end of the calendar year or if the account was closed during the year, the closure of the account. The Information to be reported is to be reported annually.

In case of inadequate information problem occurs, as the provided document through the online step-by-step procedure are not applicable or valid, the Back Office (on-boarding) and Customer Support Department ensures that the missing documentation / information are obtained during the business relationship with the Client. The Back Office (on-boarding) and Customer Support Department is aware of the missing documentation and is responsible for flagging in the system that there are missing documents.

Scope of the Application Form:

Potential Clients must submit a duly completed "Application Form" through the Company's website. This is a multi-faceted document, that apart from being used for the collection of information for AML purposes, it is also used to collect information about the investment objectives, the financial status and the knowledge and experience of the applicant, concepts of appropriateness and suitability (see ANNEX IX).

All the answers provided on the form and which relate to AML, are entered by the Back Office/ Support Department and in the specially designed database of the Company's CRM, (the database has full access controls and audit trail functionality).

The AMLCO examining the case applies the Risk Categorization principles after examining all the available information and after reviewing the documents that have been submitted as regards the identity of the Client or the beneficial owner.

Upon completing the process, the Compliance Officer asks from the Head of Back Office (on-boarding) to open the account and notifies to the same:

- The Risk Classification of the customer (Low / Medium / High)
- The Customer Due Diligence method (described in section 6)
- The MiFID II categorization (Retail, Professional or Eligible Counterparty)

5.1 The Risk Classification of the customer (Low / Medium / High)

Basing on the assessment of the information provided by the Client as well as the information obtained from other available resources during compliance checks, each of the existing or prospective Client of the Company is classified into one of the three categories, depending on the assessed level of risks possibly associated with business relationship with such Client – Low Risk, Normal Risk and High Risk.

LOW RISK CLIENTS

Low Risk Customers, according to legislation are:

- Credit or financial institutions covered by the EU Directive;
- Credit or financial institutions carrying out one or more of the financial business activities as these are defined in section 2 of the EU Directive and which are situated in a country outside the European Economic Area, which:
- In accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing, imposes requirements equivalent to those laid down by the EU Directive and
- It is under supervision for compliance with those requirements.
- Listed companies whose securities are admitted to trading on a regulated market in a country of the European Economic Area or in a third country which is subject to disclosure requirements consistent with community legislation;
- Domestic public authorities of countries of the European Economic Area. No other Entity can be considered as a Low Risk.

NORMAL RISK CLIENTS

Normal (or Medium) Risk Customers are customers that generally do not fall in the Low or High-Risk Categories. The Clients classified into this category do not represent any significant risks for a Company. They may include persons registered or domiciled in third countries, offshore and former offshore jurisdictions, clients without any track record of their activities, newly registered companies.

HIGH RISK CLIENTS

Customers are classified as high risk according to the following criteria:

- High Risk Countries & Deficient Jurisdictions: Even though literally all countries have enacted anti-money laundering legislation, the tenacity and effectiveness of implementation varies widely across jurisdictions. Deficient jurisdictions have been defined as all those countries and territories identified by the Financial Action Task Force (FATF) as non-cooperative countries and territories (NCCT) in the fight against money laundering or as having material deficiencies in their anti-money laundering procedures (see ANNEX I);
- Politically Exposed Persons (PEPs);
- Personal asset- holding vehicles, such as trusts, foundations, holdings;
- Bearer Shares: The ownership structure contains legal entities that have either issued bearer shares, their Articles and Memorandum of Association allow the issue of bearer shares and / or the switch from registered to bearer shares and / or company's shares are in bearer form.
- The Customer has not been physically present for identification purposes (non-face to face transactions) without certain safeguard, such as electronic signatures and/or not residing in a low-risk jurisdiction (see ANNEX I) in accordance with Annex II of the Law and Annex II of Directive 2015/849;
- The Corporate structure that favors anonymity, nominee shareholders;
- There are multiple accounts which have the same person(s) as beneficial owner(s): This does not necessarily imply that the accounts are used to launder money, but, it does make it easier to churn assets through accounts that are controlled by the same person, which also increases the risk of market manipulation. This criterion should be used alongside the presence of any of the other criteria mentioned hereabove;
- Unknown or unassociated third-party payments.

The above list is indicative, and it is not exhaustive. The Compliance Officer examining the case, can classify a Client (potential or existing) as high risk if there are any circumstances that would warrant so such as the industry in which the customer operates, reputational factors and other risk presented from a potential cooperation.

It is not prohibited for the Company to accept the Clients transactions with whom impose the higher risks of money laundering however, the Company must additionally apply the specific client identification due diligence procedures in regard of those Clients.

These enhanced procedures, depending of the type of the Client, are the following:

Clients whose representatives are not physically present at the stage of establishment of business relationship (non- face to

face clients):

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

- Original, or
- True copy of the original, where the certification is made by the Company in cases where it establishes the customer's identity itself, once the original is presented thereto, or
- True copy of the original, where the certification is made by third parties, in cases where they establish the customer's identity, pursuant to Article 67 of the Law and the provisions of paragraph 25 of the AML Directive, or
- True copy of the original, where the certification is made by a competent authority or person that, pursuant to the relevant provisions of the laws of their country, is responsible to certify the authenticity of documents or information, in cases where they establish the customer's identity themselves, or
- Copy of the original, provided that at least one of the procedures referred to in the next paragraph is followed.

Other possible practical procedures are as follows:

- Ensure that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution which operates in a country within the European Economic Area.
- The first payment of the operations is carried out through an account opened in the a third country, which, according to the Regulatory decision, imposes requirements on combating money laundering equivalent to those of the EU Directive.
- A direct confirmation of the establishment of a business relationship is obtained through direct personal contact, as well as, the true name, address and passport/identity card number of the customer, from a credit institution or a financial institution with which the customer cooperates, operating in a Member State or in a Third Country, which, according to the Regulatory decision, imposes requirements on combating money laundering equivalent to those of the EU Directive (or a true copy of the confirmation).
- Telephone contact with the customer at his home or office, on a telephone number which has been verified from independent and reliable sources. During the telephone contact, the Company shall confirm additional aspects of the identity information submitted by the customer during the procedure of opening his account.
- Communication with the customer through at an address that the Company has previously verified from independent and reliable sources, in the form of a registered letter.

The Company shall also apply to companies or other legal persons requesting to establish a business relationship or an occasional transaction by mail, telephone or through the internet. The Company shall take additional measures to ensure that the companies or other legal persons operate from the address of their main offices and carry out legitimate activities in all respects.

Legal persons with shares in a bearer form:

- The Company itself takes physical custody of the bearer share certificates while the business relationship is maintained or obtains a confirmation from a bank operating in the Republic of Cyprus or a country of the European Economic Area that it has under its own custody the bearer share certificates and, in case of transferring their ownership to another person, shall inform the Company accordingly,
- The account of such Client is closely monitored throughout its operation; at least once a year, a review of the accounts' transactions and turnover is carried out and a note is prepared summarising the results of the review, which must be kept in the Client's file,
- At least once every year, the official representative, director, or auditor of the Client confirms that the shareholding structure of the Client or that of its holding company (if any) has not been altered by the issue of new bearer shares or the cancellation of existing ones,
- When there is a change to the beneficial owners, the Company examines whether or not to permit the continuance of the account's operation.

Politically exposed persons:

- The Company has put in place appropriate risk management systems, including risk-based procedures to enable it to determine whether a prospective Client is a politically exposed person. Such procedures include, depending on the degree of risk, the acquisition and installation of a reliable commercial electronic database for politically exposed

persons, seeking and obtaining information from the Client himself and from publicly available sources of information. In the case of legal entities, the procedures aim at verifying whether the beneficial owners, authorised signatories and persons authorised to act on behalf of the legal entities are politically exposed persons,

- The decision for establishment of a business relationship or the execution of an occasional transaction with a politically exposed person is taken by the Director of the Company and this decision is forwarded to the Money Laundering Compliance Officer. Similarly, in case when in the process of establishment, a business relationship with a client (natural or legal person) it is subsequently ascertained that the persons involved are or have become politically exposed persons, then an approval is given for continuing the operation of the business relationship by the Director of the Company which is then forwarded to the Money Laundering Compliance Officer,
- Before establishment a business relationship or execution of an occasional transaction with a politically exposed person, the Company must obtain adequate documentation to ascertain not only the identity of the said person but also to assess his business reputation (reference letters from third parties, search of available reliable information),
- As well as with all other categories of existing or potential clients, the Company must create the economic profile of the client by obtaining the information from the Client. The details of the expected business and nature of activities of the Client form the basis for the future monitoring of the account. The profile should be regularly reviewed and updated with new data and information. The Company must be particularly cautious where its clients or beneficial owners are involved in /have links to businesses which appear to be most vulnerable to corruption and ML/TF risks, such as trading in bullions, oil, arms, cigarettes and alcoholic drinks, construction, pharmaceuticals and healthcare, Money Service Businesses, casinos, dealers in precious metals.
- The account is subject to annual review in order to determine whether to allow its continuance of operation. A short report is prepared summarising the results of the review by the Money Laundering Compliance Officer. The report is submitted for consideration and approval to the Board of Directors and filed in the client's personal file.
- The requirements of Article 64(c)(ii)(cc) of the Law, where a politically exposed person is no longer entrusted with a prominent public function by the Republic or a member state or a third country, or with a prominent public function by an international organization, the Company shall take into account the continuing risk posed by that person and applies appropriate and risk-sensitive measures for at least 12 months, until that person is deemed to pose no further risk to politically exposed persons. Such report is submitted for consideration and approval to the Board of Directors and filed in the client's personal file.

Legal persons in a form of trusts:

- When the Company establishes a business relationship or carries out an occasional transaction with trusts, it must ascertain the legal substance, the name and the date of establishment of the trust and verify the identity of the trustor, trustee and beneficial owners, according to the client identification procedures applicable to all Clients,
- Additionally, the Company must ascertain the nature of activities and the purpose of establishment of the trust as well as the source and origin of funds requesting the relevant extracts from the trust deed and any other relevant information from the trustees. All relevant data and information should be recorded and kept in the client's file.

Clients registered or domiciled in the countries which do not sufficiently apply the FATF recommendations:

The Financial Action Task Force's («FATF») Recommendations constitute the primary internationally recognised standards for the prevention and detection of money laundering and terrorist financing.

In regard of the Clients registered or domiciled in the countries which do not sufficiently apply the FATF recommendations the Company must apply the following additional procedures:

- Exercise of additional monitoring procedures paying special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or apply inadequately the FATF recommendations,
- Transactions with persons from the said countries, for which there is no apparent economic or visible lawful purpose, are further examined for the establishment of their economic, business or investment background and purpose. If the Company cannot be fully satisfied as to the legitimacy of a transaction, then a suspicious transaction report is filed to MOKAS.

With the aim of implementation of the above procedures, Money Laundering Compliance Officer consults the country assessment reports prepared by the FATF, other regional bodies that have been established and perform their activities basing on the principles of FATF. Based on the said reports, AMLCO assesses the risk from transactions and business relationships with persons from various countries and decides, whether a certain country applies the FATF's recommendations inadequately. In accordance with this decision of the Money Laundering Compliance Officer, the necessary, enhanced due diligence measures for identifying and monitoring Company must apply, when deemed transactions of persons originating from countries with significant shortcomings in their legal and administrative systems for the prevention of money laundering and terrorist financing.

5.2 Customer Adoption – Performance by third parties

Subject to certain conditions pertaining, the Company may rely on the performance by third parties (including affiliated entities) for some or all the elements of its Customer Identification process. The implementation of customer identification and due diligence procedures, as these are prescribed in sections 61(1)(a), (b) and (c) of Law L13(I)/2018, provide that the third person makes immediately available to the Company all data and information that was collected for the performance of the Customer Due Diligence process, which must be certified as true copies of the originals.

The Company shall obtain data and information to verify that the third party is subjected to professional registration and in accordance with relevant laws of its country of incorporation and/or operation as well as supervision for the purposes of compliance with the measures for the prevention of money laundering and terrorist financing.

The Company may rely on third parties only at the outset of establishing a business relationship or the execution of an occasional transaction for the purpose of verifying the identity of its customers. Any additional data and information, according to the degree of risk, for the purpose of updating the Client's economic profile or for the purpose of examining unusual transactions executed through the account, shall be obtained directly 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 the customer's funds and assets.

Where the third party is an accountant, an independent legal professional, or a trust and company services provider from a country which is a member of the European Economic Area or a third country that the Advisory Authority for Combating Money Laundering and Terrorist Financing has determined to be applying procedures and measures for the prevention of money laundering and terrorist financing equivalent to the European Union Directive, then the Company, before accepting the customer identification data verified by the said third party, shall apply the following additional measures/procedures:

a. assessment and evaluation of the systems and procedures for the prevention of money laundering and terrorist financing applied by the third party;
b. the commencement of the cooperation with the third party and the acceptance of customer identification data verified by the third party is subject to approval by the Compliance Officer or the General Manager accordingly.

06 CLIENT IDENTIFICATION AND DUE DILIGENCE PROCEDURES

Following the provisions of Applicable Legislation, the Company must perform the obligatory identification of each Client and verification of identity of each Client and, where applicable, its beneficial owners **before** the establishment of a business relationship or the carrying out of the transaction. By way of exemption to the general rule, and subject to the controls outlined here below, it is possible to allow the verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship, if this is necessary in order not to interrupt the normal contact of business and/or where there is a little risk of money laundering or terrorist financing accruing;, in which case, the procedures must be completed as soon as practicable after the initial contact and not later than 15 calendar days. Exemptions can only be granted by the Compliance Function or the Designated Board Member only for the following cases:

a. Where the potential customer is classified as "Low Risk" or "Normal Risk";
b. Following the "sign-off" by the AMLCO and/or the Designated Board Member of a special form stating the grounds for the exemption, the items of missing information and the deadline for submission of the missing documents / information;
c. If the deadline for delivery of the missing documents / information is not met, the Back Office (on-boarding) officer notifies immediately the Head of Back Office (on-boarding) Department and AMLCO or the Designated Board Member accordingly, who decides on further steps.

The keeping of anonymous accounts is strictly prohibited.

No accounts are opened with "shell banks" as these are defined within EU Legislation. No transactions are conducted with or on behalf of shell banks.

The Company does not allow any transactions with/on behalf of the customer prior to the verification process is completed, though Applicable Legislation allows such transactions during the verification of the identity of customers and beneficial owners under certain conditions.

The Due Diligence Procedures are applied:

- When establishing a business relationship;
- When carrying out occasional transactions amounting to €2.000 or more, irrespective of whether the transaction is carried out in a single operation or in several operations which appear to be linked;

- When there is suspicion of money laundering or terrorist financing, irrespective of the value of the envisaged transaction;
- When there are doubts about the veracity or adequacy of previously obtained customer identification data.
- Client identification procedures and client due diligence measures comprise (where applicable):
- Collection from the Client or Counterparty of all the documents required for its identification in accordance with the lists developed by the Company, depending on the legal form of the Client and types of business relationship,
- Identifying the client and verifying the client's identity based on documents, data or information obtained from a reliable and independent source,
- Where applicable, identifying the beneficial owner and taking risk-based and adequate measures to verify the identity on the basis of documents, data or information obtained from a reliable and independent source so that the Company knows who the beneficial owner is; as regards legal persons, trusts and similar legal arrangements, taking risk based and adequate measures to understand the ownership and control structure of the client,
- Obtaining information on the purpose and intended nature of the business relationship,
- Creation of an economic profile for the customer/beneficial owner (in accordance with requirements of legislation, current Manual and Company's Internal Operation Manual),
- Carrying out a suitability and/or appropriateness test for the customer/beneficial owner (in accordance with requirements of legislation and Company's Internal Operation Manual),
- Conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the information and data in the possession of the Company in relation to the client, the business and risk profile, including where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

Responsible Department for KY & Approval of clients:

All of the Client's documents should be uploaded online or sent via email to compliance@nbhm.eu and then an assigned representative checks the respective documents. If all documents are received, the Client is being Submitted for approval but if a document is missing or the Clients skips the document upload, the representative contacts the Client and collect all necessary documentation, uploading it to the client's profile, and submits the client for approval. The checking process is started by Back office and client approved/rejected.

1. Proof of Identity (POI):
   Proof of Identity documents must include the following information:

- Number of the document
- Full Name
- Photo
- Date of birth
- Date of issue
- Date of expiry
- Signature

When reviewing proof of identity, the responsible person must:

- Ensure that the document is authentic and not modified;
- Compare the details registered in CRM and ensure they are matching with the provided POI;
- Confirm that the quality of the document is sufficient.

Acceptable proof of identities (POI):

I. Passport:
   - Color copy and valid (not expired)'
   - The copy should be provided in a way that its boarders are visible, including all the numbers (2 lines) at the bottom.

II. Identification Card and Driving License:
   - When an ID is provided, a DL should be requested, too as an enhanced due diligence measure;
   - A clear color copy of the front and back with all corners of the document, all the numbers should be in place;
   - Valid (not expired).

In case where the ID is approved but the DL is expired, the client must provide proof of renewal request or temporary DL.

2. Proof of Address (POA):
   Proof of address documents must include the following information:

- Full name of the client,
- Full residence address,

- Date of issue,
- Issuing company/institution (name, logo, stamp or at least details of the company/institution)

When reviewing proof of address documents, the responsible person must:
- Ensure that the document is authentic and not modified;
- Ensure that the date of issue is in 3 months and not older than 6 months;

Acceptable proof of addresses:
- Utility bill, such as electricity, water, landline telephone and internet;
- Tax statement;
- Insurance;
- Bank Statement.

3. Proof of Payment:
   Payment options:
   I. Credit/Debit Card:
      - Copy of card (front and back).
      - The front should present the last 4 digits (client should hide the rest).
      - The client should hide the CVV code.
      - The front should include the client name and the expiration date.
      - The card must be signed.

   II. Wire transfer:
      - Swift/BIC copy.

   III. Shared wallets such as Skrill etc.:
      - Screenshot of the transaction including client's name, account number and transaction amount.

If any of the documents provided is not in English language, translation form must be prepared and attached together with the document.

Steps to accepting and activating clients:

I. Client registers,
II. Client deposits,
III. Partial activation:

This means the client can trade for up to 15 days from initial deposit with partial KYC and only up to 2,000 EUR/USD deposit.

In the case where over 2,000 EUR/USD is deposited, the company shall block the client from trading, close positions and refund the client the remaining balance.

Partial activation requirements:
- Application form is completed,
- ONE KYC document is provided, either POI or POR.

The Client will be given up to 15 calendar days to provide FULL KYC documents as described through this manual.

Failure to provide FULL KYC documents within 15 calendar days will lead to closure of any open positions and refund of the closing balance after withdrawal fees.

Once the Client has provided FULL KYC documents, they will be set to full compliance and can deposit over 2,000 EUR/USD.

Declaration of Deposit MUST be obtained through the business relationship with the Client.

The 15 Days' warning notice will be sent in the following order:
- 1st reminder will be sent from Back Office to the Support and/or Sales desk within 7 days of the first-time deposit, saying that the Client has only one week left to verify the account.
- 2nd warning will be sent from Back Office to the Support and/or Sales desk within 13 days of the first-time deposit.
- The Support department will provide their comments to the Risk Department, the Designated Board Member and the AMLCO.
- Last warning with all updates will be sent to all relevant departments at the morning of the 15th day with reminder that the client will be refunded by 18:00 at latest.

If the client fails to comply then his account MUST be closed, and the outstanding balance shall be returned to the same source from where the Company received the deposit.

6.1 Non-compliance Clients

Failure or refusal by a client to submit, before the establishment of a business relationship or the execution of an occasional transaction, the requisite data and information for the verification of his identity and the creation of his economic profile, without adequate justification, constitutes elements that may lead to the creation of a suspicion that the client is involved in money laundering or terrorist financing activities. In such an event, the Company does not proceed with the establishment of the business relationship or the execution of the occasional transaction while at the same time the Money Laundering Compliance Officer considers whether it is justified under the circumstances to submit a report to MOKAS.

If, during the business relationship, a client fails or refuses to submit, within a reasonable timeframe, the required verification data and information, the Company terminates the business relationship and closes all the accounts of the client while at the same time examines whether it is justified under the circumstances to submit a report to MOKAS.

6.2 Construction of Client's economic profile

Before the establishment of the business relationship and during the identification of customer/beneficial owner, the data and information are collected from the Client, with the aim of constructing the client's economic profile and, as a minimum, include the following:

- The purpose and the reason for requesting the establishment of a business relationship,
- The anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments,
- The client's size of wealth and annual income and the clear description of the main business/professional activities/operations.

The data and information that are used for the construction of the client's-legal person's economic profile include, but are not limited to, the name of the company, the country of its incorporation, the head offices address, the names and the identification information of the beneficial owners, directors and authorised signatories, financial information, ownership structure of the group that the company may be a part of (country of incorporation of the parent company, subsidiary companies and associate companies, main activities and financial information). The said data and information are recorded in a separate form designed for this purpose which is retained in the client's file along with all other documents. The said form is updated regularly or whenever new information emerges that needs to be added to the economic profile of the client or alters existing information that makes up the economic profile of the client. In the case of a client-natural person, the Company obtains data and information identical with the abovementioned and in general, the same procedures that are followed.

The Company is satisfied that it is dealing with a real person and, for this reason, obtains sufficient evidence of identity to verify that the person is who he/she claims to be. Furthermore, the Company verifies the identity of the beneficial owners of the Clients' accounts. In the cases of legal persons, the Company obtains adequate data and information to understand the ownership and control structure of the Client. Irrespective of the customer's type (e.g. natural or legal person, sole trader or partnership), the Company requests and obtains sufficient data and information regarding the customer's business activities and the expected pattern and level of transactions.

A profile is created for each new Client that contains all relevant KYC information in hard copy and the Compliance Function is responsible for the keeping and updating of the folder. In addition, all documents submitted by the Client are scanned and stored in electronic format on a designated directory on the Company's servers.

Form called "Personal Meeting Note" and "Skype Video Call Note" can be as an additional confirmation of Face-to-Face meeting [Annex III, point (c) of the Fifth Anti Money Laundering Directive (EU) 2018/843] with the prospective or existing clients or any other person that has an intention to conduct the business relationship with the company (such as an Introducing Broker or similar). In order to categorise client as Face-to-Face the employee who held a meeting must notify AMLCO about past meeting by e-mail. When true copy of clients' document provided after face-to-face meetings, On-boarding Department upload scan-copies to clients' profiles and store the true-copy documentation.

The Client's profile is frequently updated throughout the operation of the account and all the information contained therein, and other information related to the operation of the account that is kept in electronic form is retained for a period of five years after the business relationship with the Customer has ended or the last transaction was carried- out.

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.

Identification of the Beneficial Owners

Beneficial Owner is defined as the natural person(s) who ultimately owns or controls the customer and / or the natural person

on whose behalf a transaction or activity is being conducted and includes at least the following for:

1. **Legal entities (companies):**
   a. the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards which ensure adequate transparency of ownership information; a percentage of 25% plus one share shall be deemed sufficient to meet this criterion;
   b. the natural person(s) who otherwise exercises control over the management of a legal entity.
   c. the natural person who holds the position of senior managing official if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under subsection a) and b) of the present section is identified, or if there is any doubt that the person identified is the beneficial owner; provided that the Company took actions in order to identify the beneficial ownership and recorded these actions.
2. **Foundations, and legal arrangements, such as trusts, which administer and distribute funds:**
   a. where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25% or more of the property of a legal arrangement or entity;
   b. where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;
   c. the natural person(s) who exercises control over 25% or more of the property of a legal arrangement or entity.
3. **Special cases:**
   a. Collective Investment Vehicles: The definition refers to unit trusts, mutual funds and hedge funds. Because in such cases, the number of beneficial owners is potentially large and because the beneficial owners change continuously, the Customer Due Diligence process is performed for the Investment Manager or the Administrator of the fund.

   In such cases, before Company apply this exemption, we need to collect sufficient proof of the fact that the Client belongs to this category. Such information might consist of:
   - Copy of the prospectus
   - Articles and Memorandum of Association

   In addition, the business relationship between the fund and the Fund Manager or the Administrator must also be established. This can be achieved by obtaining extracts of the management agreement between the fund and the Fund Manager or the Administrator.

   b. Situations where the Client specifies explicitly the counterparty to the transaction: According to Circular 2007/12 issued by CySEC, if a Client submits an order for execution and at the same time specifies explicitly who the counterparty in the transaction is going to be, the Company is obliged to carry-out the same Customer Due Diligence procedures that are applied for our Clients in respect of the specified counterparty in the transaction. The logic behind this requirement is that it would be a convenient way for a money launderer to blur the trail of the money by making transactions between a number of companies that are in effect controlled by the same, without losing beneficial ownership of the assets. It would also be a convenient way to abuse the markets by either creating plasmatic prices and/ or volumes.
   c. Transactions on behalf of a third party: The Company is obliged to take adequate measures for the collection of sufficient documents, information or data for the identification and verification of the identity of any third person on whose behalf the Client is acting.
   In addition, for customers that are corporate entities or other legal entities such as foundations and legal arrangements such as trusts, it must be verified that the natural person(s) that purports to act on behalf of the Client is duly authorized for that purpose and the identity of such persons must be established and verified.

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

A person's residential and business address is an essential part of his/her identity and, thus, a separate procedure for its verification, is followed. It is never acceptable to use the same verification data or information for verifying the customer's identity and verifying its home address.

In addition, the validity and the authenticity of the Client's documents collected is checked and performed through the World Compliance Check.

The AMLCO is responsible for establishing the data and information collected by the Customer Support Department

before the establishment of a business relationship, with the aim of constructing the Client's economic profile. These include the following:

a. the purpose and the reason for requesting the establishment of a business relationship;
b. the anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments;
c. the customer's size of wealth and annual income and the clear description of the main business/professional activities/operations.

The information requested for various categories of Clients is based on the Applicable Legislation. The AMLCO and the Head of Customer Support Department ensure that the information collected for each category of Client is as per requirements. The AMLCO may also obtain information from outside sources where deemed necessary.

In cases where:

a. Any Client fails or refuses to submit the required data and information without adequate justification then this might lead to the creation of a suspicion that the customer is involved in money laundering or terrorist financing activities. In this case, the Company does not proceed with the establishment of the business relationship or the execution of the occasional transaction while at the same time the AMLCO considers whether it is justified under the circumstances to submit a report to MOKAS.
b. If, during the business relationship, a customer fails or refuses to submit, within a reasonable timeframe (15 days), the required verification data and information for the verification of their identity and the creation or update of their economic profile, the Company terminates the business relationship and closes all the accounts of the customer at the same time examines whether it is justified under the circumstances to submit a report to MOKAS.
c. If, during establishment of cooperation some pending issues left for the KYC procedure, a maximum amount of deposited funds limited at €2,000 and a maximum 15-day timeframe to complete the customer's identity verification process. If this is not verified within 15 days, the Company is obliged to terminate the business relationship and return deposited funds to the customer to the bank account of origin immediately.

All Client applications are approved by the Head of Customer Support Department and the AMLCO.
Factors that might lead the AMLCO to reject or examine more thoroughly an application, include the following:

a. Transactions executed are much larger than the anticipated account's turnover or are not justified by the available information on the customer. For example, the amount of capital that the Client wishes to invest is larger than expected with respect of his/her income;
b. The sources of the investment capital are unclear;
c. The distance separating the reported residence and work addresses is large;
d. The Client:
    - avoids providing client due diligence information;
    - avoids giving clear information regarding his/her professional activities;
    - avoids personal contact and meetings;
    - provides information which is either difficult or impossible to verify;
    - holds accounts in many financial services companies;
    - lives/ works in a country considered to be a "tax haven".

The presence of the above does not define the Client as a suspect case, but if he/she is a new, unknown, and has approached the Company without sufficient references, then the Company shall have to act with care in examining the application.

The client due diligence measures and identification procedures are obligatory for each Client, however, the Company may determine the extent of such measures on a risk-sensitive basis depending on the type of client, business relationship, product or transaction, provided the Company is able to demonstrate to the competent Supervisory Authorities that the extent of measures is appropriate in view of the risks of the use of its services for the purposes of money laundering and terrorist financing.

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

- It is reasonably possible to establish that the client is the persons he claims to be, and
- The Company is satisfied that the client is the person he claims to be.

No single form of identification can be fully guaranteed as genuine or representing correct identity and, consequently, the identification process will generally need to be cumulative. Verification of the clients' identity is based on reliable data and information issued or obtained from independent and reliable sources, meaning those data, and information are the most difficult to be amended or obtained illicitly.

A person's residential and business address is an essential part of his identity and, thus, a separate procedure for its

verification must be followed. It is never acceptable to use the same verification data or information for verifying the client's identity and verifying its home address.

Specific Customer Identification Procedures

Specific Customer Identification Procedures and Information Requested from Different Categories of Clients. Based on Directive DI144-2007-08 of 2012 of the Cyprus Securities and Exchange Commission for the Prevention of Money Laundering and Terrorist Financing and the relevant Law the following Customer Identification Procedures are applied within the Company:

1. **Natural Persons Residing in the Republic**
   a. The Company ascertains the true identity of natural persons who are residents of the Republic Cyprus by obtaining the following information:
      - true name and/or names used as these are sated on the official identity card or passport,
      - full permanent address in the Republic, including postal code,
      - telephone (home and mobile) and fax numbers,
      - e-mail address, if any,
      - date and place of birth,
      - nationality and
      - details of the profession and other occupations of the customer including the name of employer/business organization.

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

   c. In addition to the name verification, it is important that the customer's permanent address is also verified by using one of the following ways:
      - visit at the place of residence (in such a case, the Company's officer who carries out the visit prepares a memo which is retained in the customer's file), and
      - the production of a recent (up to 6 months) utility bill, local authority tax bill or a bank statement or any other document same with the aforesaid (to protect against forged or counterfeit documents, the prospective customers are required to produce original documents).

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

2. **Natural Persons Not Residing in the Republic**
   a. For customers who are not normally residing in the Republic, in addition to the information collected according to point (1) of the present Specific Customer Identification Procedures, the Company, without prejudice to the application on a risk sensitive basis, requires and receives information on public positions which the prospective customer holds or held in the last twelve months as well as whether he is a close relative or associate of such individual, in order to verify if the customer is a politically exposed person, according to point (5) of the Fourth Appendix of the Directive.

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

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

3. **Joint Accounts**

In the cases of joint accounts of two or more persons, the identity of all individuals that hold or have the right to manage the account, are verified according to the procedures set in points (1) and (2) of the present Specific Customer Identification Procedures.

4. Accounts of Unions, Societies, Clubs, Provident Funds and Charities

In the case of accounts in the name of unions, societies, provident funds and charities, the Company ascertains their purpose of operation and verifies their legitimacy by requesting the production of the articles and memorandum of association/procedure rules and registration documents with the competent governmental authorities (in case the law requires such registration). Furthermore, the Company obtains a list of the members of board of directors/management committee of the abovementioned organizations and verifies the identity of all individuals that have been authorized to manage the account according to the procedures set in points (1) and (2) of the present Specific Customer Identification Procedures.

5. Accounts of Unincorporated Businesses, Partnerships and Other Persons with No Legal Substance

a. In the case of unincorporated businesses, partnerships and other persons with no legal substance, the identity of the directors, partners, beneficial owners and other individuals who are authorised to manage the account is verified according to the procedures set in points (1) and (2) of the present Specific Customer Identification Procedures. In addition, in the case of partnerships, the original or a certified true copy of the partnership's registration certificate is obtained.

b. The Company obtains documentary evidence of the head office address of the business, ascertains the nature and size of its activities and receives all the information required according to paragraph 21 of the Directive for the creation of the economic profile of the business.

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

6. Accounts of Legal Persons

a. For customers that are legal persons, it is established that the natural person appearing to act on their behalf, is appropriately authorized to do so and his identity is established and verified according to the procedures set in points (1) and (2) of the present Specific Customer Identification Procedures.

b. The Company takes all necessary measures for the full ascertainment of the legal person's control and ownership structure as well as the verification of the identity of the natural persons who are the beneficial owners and exercise control over the legal person.

c. The verification of the identification of a legal person that requests the establishment of a business relationship or the execution of an occasional transaction, comprises the ascertainment of the following:

- the registered number,
- the registered corporate name and trading name used,
- the full addresses of the registered office and the head offices,
- the telephone numbers, fax numbers and e-mail address,
- the members of the board of directors,
- the individuals that are duly authorized to operate the account and to act on behalf of the legal person,
- the beneficial owners of private companies and public companies that are not listed in a regulated market of a European Economic Area country or a third country with equivalent disclosure and transparency requirements.
- the registered shareholders that act as nominees of the beneficial owners,
- The economic profile of the legal person, according to the provisions of paragraph 21 of the Directive

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

- certificate of incorporation and certificate of good standing of the legal person,
- certificate of registered office,
- certificate of directors and secretary,
- certificate of registered shareholders in the case of private companies and public companies that are not listed in a regulated market of a European Economic Area country or a third country with equivalent disclosure and transparency requirements,
- certificate of good standing (issued within the last six months)
- memorandum and articles of association of the legal person,
- a resolution of the board of directors of the legal person for the opening of the account and granting authority to those who will operate it,

- in the cases where the registered shareholders act as nominees of the beneficial owners, a copy of the trust deed/agreement concluded between the nominee shareholder and the beneficial owner, by virtue of which the registration of the shares on the nominee shareholder's name on behalf of the beneficial owner has been agreed.
- documents and data for the verification, according to the provisions of the present Directive, the identity of the persons that are authorized by the legal person to operate the account, as well as the registered shareholders and beneficial owners of the legal person.

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

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

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

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

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

i. Apart from verifying the identity of the beneficial owners, the Law requires that the persons who have the ultimate control over the legal person's business and assets are identified. In the cases that the ultimate control rests with the persons who have the power to manage the funds, accounts or investments of the legal person without requiring authorization and who would be in a position to override the internal procedures of the legal person, the Company, verifies the identity of the natural persons who exercise ultimate control as described above even if those persons have no direct or indirect interest or an interest of less than 25% in the legal person's ordinary share capital or voting rights.

j. In cases where the beneficial owner of a legal person, requesting the establishment of a business relationship or the execution of an occasional transaction, is a trust set up in the Republic or abroad, the Company must ascertain in a legal substance, the name and the date of establishment of the trust and verify the identity of the trustor, trusty and beneficial owners according to the customer identification procedures prescribed in the Law.

7. Investment Funds, Mutual Funds and Firms Providing Financial or Investment Services

a. Without prejudice of the provisions of the Law, the Company may establish and maintain business relationships or execute occasional transactions with persons who carry out the above services and activities which are incorporated and/or operating in countries of the European Economic Area or a third country which according to a decision of the Advisory Authority for Combating Money Laundering Offences and Terrorist Financing it has been determined that applies requirements equivalent to those laid down in the European Union Directive, provided that:

- the said persons possess the necessary license or authorization from a competent supervisory/regulatory authority of the country of their incorporation and operation to provide the said services, and
- are subject to supervision for the prevention of money laundering and terrorist financing purposes.

b. In the case of the establishment of a business relationship or the execution of an occasional transaction with persons who carry out the above services and activities and which are incorporated and/or operating in a third country other than those mentioned in point (a) above, the Company requests and obtains, in addition to the abovementioned, in previous points, documentation and the information required by the present Directive for the identification and verification of persons, including the beneficial owners, the following:

- a copy of the license or authorization granted to the said person from a competent supervisory/regulatory authority of its country of incorporation and operation, whose authenticity should be verified either directly with the relevant supervisory/regulatory authority or from other independent and reliable sources, and
- adequate documentation and sufficient information to fully understand the control structure and management of the business activities as well as the nature of the services and activities provided by the customer.

c. In the case of investment funds and mutual funds the Company, apart from identifying beneficial owners, obtains information regarding their objectives and control structure, including documentation and information for the verification of the identity of investment managers, investment advisors, administrators and custodians.

8. Nominees or Agents of Third Persons

a. The Company takes reasonable measures to obtain adequate documents, data or information for the purpose of establishing and verifying the identity, according to the procedures set in the previous points of the present Specific Customer Identification Procedures:

- the nominee or the agent of the third person, and
- any third person on whose behalf the nominee or the agent is acting.

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

In addition to the client due diligence measures and identification procedures, the Company ensures that the client identification records remain completely updated with all relevant identification data and information throughout the business relationship. The Company examines and checks, on a regular, and at least annual, basis, the validity and adequacy of the client identification data and information it maintains, especially those concerning high risk clients. The results of these regular reviews are recorded in reliable notes should be kept in the respective client file.

If at any time during the business relationship the Company becomes aware that reliable or adequate data and information are missing from the identity and the economic profile of the client, then it must take all necessary actions, by applying the client identification and due diligence procedures to collect the missing data and information, the soonest possible, so as to identify the client and update and complete the client's economic profile, taking into consideration the level of inherent risks.

In addition to the above procedures, the Company checks the adequacy of the data and information of the client's identity and economic profile, whenever one of the following events or incidents occurs:

- An important transaction takes place which appears to be unusual compared to the normal pattern of transactions and the economic profile of the client;
- A material changes in the client's legal status and situation, such as:
  - Change of directors/ secretary,
  - Change of registered shareholders and/ or beneficial owners,
  - Change of registered office,
  - Change of trustees,
  - Change of corporate name and/ or trading name,
  - Change of the principal trading partners and/ or undertaking of new major business activities,
  - A material change in the way and the rules the client's account is operated, such as:
  - Change in the persons that are authorised to operate the account,
  - Application for the opening of new account for the provision of new investment services and/ or Financial Instruments.

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

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

6.3 Simplified client identification and due diligence procedures

According to section 63 of Law L13(I)/2018, the Company may apply simplified customer due diligence measures, so long as it has previously ensured that the business relationship or the transaction presents a lower risk. In accordance with the requirements this are the following categories of clients:

- Credit or financial institutions covered by the EU Directive,
- Credit or financial institutions which are situated in a country outside the European Economic Area, which:

a. in accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing, imposes requirements equivalent to those laid down by the EU Directive, and

b. are under supervision for compliance with those requirements,

- Listed companies whose securities are admitted to trading on a regulated market in a country of the European Economic Area or in a third country which is subject to disclosure requirements consistent with community legislation,
- Domestic public authorities of countries of the European Economic Area.

It is provided that the Company must collect sufficient information, so as to decide whether the client can be exempted according to the provisions of the Law. Such information may include the details of the client's license and registration information, analysis of applicable legislation of the client's country of domicile, as well as any relevant information obtained from available sources.

For the purposes of applying the above requirements, public authorities or public bodies of the European Economic Area countries must fulfil all the following criteria:

- The client has been entrusted with public functions pursuant to the Treaty on European Union, the Treaties on the Communities or Community secondary legislation,
- The client's identity is publicly available, transparent and certain,
- The activities of the client, as well as its accounting practices, are transparent,
- Either the client is accountable to a community institution or to the authorities of a member state or appropriate check and balance procedures exist, which ensure the control of the client's activity.

Applying simplified customer due diligence procedures does not absolve from the need to collect information about the natural persons who can commit the Client in any agreement. Such information includes:

- Certificate of Directors issued by a reliable and independent authority.
- In the case of large financial institutions where other persons, apart from the Directors, can commit the Client in its dealings with our Company.
- A Signatory List.
- Any Power of Attorneys that may have been issued by the Client to third parties representing the customer.

6.4 Enhanced client identification and due diligence procedures

Under the Law L13(I) and Directive (EU) 849/2015, the Company is required to have in place enhanced procedures where money laundering risk is high. The Company, in order to comply with the mentioned legislation, applies enhanced customer identification and due diligence methods, in respect to High-Risk Clients, as these are defined in Articles 18-24 of the Directive.

The Company recognizes that there is a heightened risk of not knowing the customer's true identity for certain types of accounts, such as an account opened in the name of an entity that is created, or conducts substantial business in, a jurisdiction that has been designated by relevant authorities as of primary money laundering concern or has been designated as non-cooperative by an international body such as the Financial Action Task Force (FATF).

Additional measures may be used to obtain information about the identity of customers that pose a heightened risk, as standard documentary methods may prove to be insufficient. Such additional procedures for verifying the identity of certain Clients would include obtaining information about individuals with authority or control over such accounts.

According to the provisions of the Directive the company **always** categorize its clients as High-Risk and applies Enhanced Due diligence measures, where:

- The client, or the client's beneficial owner is a PEP;
- Where the Company enters into a correspondent relationship with a respondent institution from a non-EEA state;
- The client is established in high-risk third countries,
- All complex and unusually large transactions, or unusual patterns of transactions, that have no obvious economic or lawful purpose.

Main but not exhaustive list of factors determining that the client could be categories as High-Risk are:

a. Customer risk factors:
   - the business relationship is conducted in unusual circumstances;
   - customers that are resident in geographical areas of higher risk;

- legal persons or arrangements that are personal asset-holding vehicles;
- companies that have nominee shareholders or shares in bearer form;
- frequent changes on due diligence or payment details;
- the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

b. Product, service, transaction or delivery risk factors:
- transactions are unusually large;
- non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;
- payment received from unknown or unassociated third parties;

c. Geographical risk factors:
- the client or their custodian is based in a jurisdiction associated with higher ML/TF risk;
- the funds come from a jurisdiction associated with higher ML/TF risk

Based on Article 18 (a) of the Fifth Anti Money Laundering Directive (EU) 2018/843, the company has enforced additional due diligence measures as:

a. obtaining additional information on the customer and on the beneficial owner(s);
b. obtaining additional information on the intended nature of the business relationship;
c. obtaining information on the source of funds and source of wealth of the customer and of the beneficial owner(s);
d. obtaining information on the reasons for the intended or performed transactions;
e. obtaining the approval of senior management for establishing or continuing the business relationship;
f. conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination. In some cases, the company may require that the first payment be carried out through an account in the customer's name with a credit institution subject to customer due diligence standards.

Customers categorized as "**High-Risk**" are subject to certain additional measures and controls. These include:

1. In cases where the Client has not been physically present for identification purposes or the customer is requesting to establish a business relationship or an occasional transaction by mail, telephone or through the internet (non-face-to-face transactions), at least one of the following measures, or a combination of them, must be applied:
   a. Obtain additional documents, data or information for verifying customer's identity.
      - a personal interview is recommended during which all information for customer identification should be obtained;
      - at least one of the following measures should be applied:
         I. The first payment of the operations is carried out through an account opened in the Client's name with a credit institution operating and licensed in a third country, which, according to the Advisory Authority's decision, imposes requirements on combating money laundering equivalent to those of the EU Directive.
         II. A direct confirmation of the establishment of a business relationship is obtained through direct personal contact, as well as, the true name, address and passport/identity card number of the customer, from a credit institution or a financial institution with which the customer cooperates, operating in a Member State or in a Third Country, which, according to the Advisory Authority's decision, imposes requirements on combating money laundering equivalent to those of the EU Directive (or a true copy of the confirmation).
         III. Telephone contact with the customer at his/her home or office, on a telephone number which has been verified from independent and reliable sources. During the telephone contact, the Company shall confirm additional aspects of the identity information submitted by the customer during the procedure of opening his/her account.
         IV. Communication via video call with the customer, provided that:
            - the video recording and screen shot safeguards apply to the communication;
            - the said customer cannot deposit an amount over €2.000 per annum, irrespective of the number of accounts that he/she keeps with the Financial Organization;

            Unless,

            - an additional measure out of the list of measures enumerated under this section is taken;

            Or,

            - any of the supplementary measures of paragraph (b) here below is taken in order to verify his/her identity.
            - The Company evaluates the results of electronic verification in order to assess that the conditions of Article 61(3) of Law L13(I)/2018 are satisfied, namely that the proof of identity is satisfactory, in the

sense that:

- it is reasonable possible to establish that the customer is the person he/she claims to be; and
- the person who examines the evidence is satisfied, in accordance with the procedures followed under the said law and this Policy, that the Client is actually the person he/she claims to be.
- The Company shall, in such cases, establish mechanisms for the carrying out of quality controls in order to assess the quality of the information on which it intends to rely upon.
- Information must come from two or more sources. The electronic verification procedure shall at least satisfy the following correlation standard:
- Identification of the Client's full name and current address from one source (Utility Bill), and
- Identification of the Client's full name and either his/her current address or date of birth from a second source (Identification document, i.e. Passport).
- For purposes of carrying out the electronic verification, the Company shall:
- Establish procedures in order to satisfy the completeness, validity and reliability of the information to which it has access;
- Ensure that the verification procedure includes a search of both positive and negative information.

b. Take supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution covered by the EU Unit for Combating Money Laundering, such as:

- Original, or
- True copy of the original, where the certification is made by the Company in cases where it establishes the customer's identity itself, once the original is presented thereto, or
- True copy of the original, where the certification is made by third parties, in cases where the customer's identity is established by relying on the performance by third parties of the customer due diligence process.
- True copy of the original, where the certification is made by a competent authority or person that, pursuant to the relevant provisions of the laws of their country, is responsible to certify the authenticity of documents or information, in cases where they establish the customer's identity themselves, or
- Copy of the original, provided that at least one of the procedures referred to in paragraph (b) is followed.

c. Ensure that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution which operates in a country within the European Economic Area.

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

d. When the client states at the application form that his initial deposit is 10,000 (ten thousand) and more, the Source of income is required.

2. In respect of Politically Exposed Persons (PEPs), at least one of the following measures, or a combination of them, must be applied:

a. The approval of the General Manager is required for establishing business relationships with PEPs.

b. The source of wealth and source of funds that are involved in the business relationship or the transaction must be established.

c. Such accounts are subjected to continuous monitoring.

3. Companies the capital of which consists of bearer shares:

As a general rule, no account should be opened for legal entities the ownership structure of which includes at least one company who has either issued bearer shares or the Articles and Memorandum of Association allows the issue of bearer shares and / or the switch from registered to bearer shares.

Information will be verified within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, the Company may refuse to complete a transaction before it has verified the information. Approval by General Manager must be obtained prior to completing a transaction when the verification of information has not been completed.

In addition, the Company may, pending verification, restrict the types of transactions or quantity of transactions as to number and/or amount invested in, until the verification of information has been fully completed.

According of Company's internal procedures Enhanced Due Diligence includes:

- Request a second proof of Identity
- MRZ check of ID document and/or passport

- KYC call
- Additional search vs. sanction lists
- Additional approval by AMLCO and Management
- Request of proof of source of funds
- Request of proof of source of wealth
- Additional management approval for internal transfer transaction when high-risk clients are involved
- Interviews
- Collection of additional information from different sources (public and non-public)

In addition, the Company and AMLCO should use different approach to ongoing monitoring of High-Risk and Medium Risk clients. High Risk profiles are checked at least twice more often than those of Medium Risk.

Combination of several such procedures are applied in each case using risk-based approach. Threshold requiring special control are also set much lower. Quantitative parameters for assessment of risk presented by High Risk clients from AML perspective are also set much higher levels.

6.5 Updating of records and record keeping

The Company applies a cascaded review process that involves the following steps:

1. The Client is contacted in appropriate time (usually 28 days) before any of the documents collected as part of the Customer Due Diligence Process expires and is asked, where applicable, to provide a copy of the renewed document (for example passport or identity card) or to inform us whether the due-to-expire instrument of authorization (e.g. Power of Attorney) will be renewed or not, and if it will be renewed, to obtain us with a copy of the renewed document. If the documents weren't provided, the Support Department is in charge to contact the client for the document request. In case it is still not provided, the client will be informed about the termination of cooperation with the company.

   Automated KYC update for existing clients in CRM implemented as following:
   - In 28 days before the expiration of the Proof of ID the e-mail sent to the client with the request of the new document. The reminder is to be sent in 14 days before the expiration. The date of the request appears in the relevant field on profile of the client in CRM. On-boarding Department receives notifications about expired Proof of ID.
   - 28 days before the expiration date, the automatic request to be sent to clients and reminder in 14 days if needed. In CRM the field "Address approved" a note with the date of automatic request appears. In personal Client's Area the Client also can see "proof of address approved" - "No" and notification to upload the new document. (When the document is expired, the field "Address approved" in CRM state as "No".)
2. A review process is performed on a regular basis. The review process has two distinctive forms, namely:

Full Review

In this case, Clients and counterparties are asked to submit recent copies of all the documents that are required for the performance of the Customer Due Diligence process, and the duly completed and updated Application Form according to the following frequency, depending of their risk categorization:

- Low-Risk accounts: Once every five (5) years
- Medium Risk accounts: Once every two (2) years
- High-Risk accounts: Every year

Soft Review

In this case, an email is sent to Clients and counterparties asking them to either confirm that the information that the Company has on record is still valid and true or otherwise to notify the Company if any of the said information has changed. In the latter scenario, the affected Client / counterparty shall submit all the necessary documents that confirm the changes. The soft reviews are performed according to the following frequency, depending on the risk categorization of each account:

- Low and Medium Risk / High-Risk accounts: Every year

The Full and Soft Review processes interact with each other in the sense that, if during any of the two schedules, it is time for an account to undergo a Full Review, the Soft Review will be substituted by the Full Review and from there on, the Soft Review process will run at the frequency that applies for the particular Client.

Notwithstanding the procedure outlined here above, Clients have a contractual obligation to notify Company in cases where there is any change in the capital structure or any other development that would bring about a change in effective control as soon as such an event occurs or becomes known to the management of the customer. The Client is also expected to notify us immediately of any termination of the authorization granted to any of the signatories / attorneys.

In the case of Clients who are classified as High-Risk, by decision of the Compliance Function and in the application of the Enhanced Due Diligence concept, additional information might be required from the Client, like a copy of the latest audited financial statement.

In the case of Clients that were classified as "Low-Risk", the updating of records is carried-out in the same manner as the at the adoption process – for example, if proof of authorization was obtained through the internet for the set-up of an account for a European regulated Investment Firm, the same will apply for the update process.

The AMLCO is responsible for keeping record of all the documents / data related to the investigation of Money Laundering activities and any reports filed to the Commission or Board of Directors of the Company.

This includes:

- Staff training records;
- Periodic operations review records;
- Reports and recommendations submitted to the Company's Board;
- Reports submitted to the Commission;
- Money laundering inquiries from the Unit;
- Money laundering reports and disclosures to the Unit.

The Company keeps record of the documents, data and information collected and/ or obtained within the scope of KYC and due diligence procedures for a period of at least 5 (five) years, which period is calculated after the carrying out of the transactions or the termination of the business relationship.

It is provided that, the documents and other data relevant to ongoing investigations are kept until MOKAS confirms that the investigation has been completed and the case has been closed.

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

When the Financial Organisation establishes a documents/ data retention policy, it shall take into consideration the requirements of the applicable legislation and the potential needs of MOKAS and the Commission.

The documents and/ or data obtained, for compliance with applicable legislation, shall be in their original form or in a certified true copy form. In the case that the documents or data are certified as true copies by a different person than the Company itself or by the relevant third person as provided for by the applicable legislation, these documents and/ or data must be apostilled or notarised.

A true translation shall be attached in the case that the documents and/ or data mentioned above are in a language other than English.

07 MONITORING OF TRANSACTIONS

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 has a full understanding of normal and reasonable account activity of its Clients and their economic profiles and has the means of identifying transactions which fall outside the regular pattern of an account's activity or of identifying the

complex or unusual transactions or transactions without obvious economic purpose or clear legitimate reason.

Monitoring of the Clients' transactions and accounts is the obligatory component of the effective management of the risk of money laundering.

The purpose of this monitoring is the identification of the following types of transactions:

- Transactions which, by their essence, may be associated with money laundering
- Unusual transactions - the transactions which have no apparent economic or visible lawful purpose, and
- Suspicious transactions - the transactions which may be considered to be inconsistent with the usual business patterns of the Client, his normal personal, trading or financial activities, his economic profile or the usual turnover of his account with the Company.

There is no exact definition or the exhaustive list of the transactions, which are deemed to be suspicious, however, the Company has identified the following examples of operations and transactions on behalf of its Clients and Counterparties that might give rise to a suspicion of their relation to money laundering or terrorist financing:

- Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the client,
- The business relationship involves only one transaction, or it has a short duration,
- Transactions which are not in line with the conditions prevailing in the market, in relation, particularly, with the size of the order and the frequency,
- Settlement of the transaction by a third person which is different than the client which has submitted the order,
- Instructions for payment in favour of a third person that does not seem to be related with the ordering Client,
- A client is reluctant to provide complete information when establishes a business relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with Company, names of its officers and directors, or information on its business location; the client provides minimum or misleading information that is difficult or expensive for the Company to verify,
- A client provides unusual or suspicious identification documents that cannot be readily verified,
- A client that 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 client - legal person,
- Unexplained inconsistencies arising during the process of identifying and verifying the client (previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents submitted to confirm name, address and date of birth),
- Complex trust or nominee network,
- Transactions or company structures established or working with an unneeded commercial way, such as 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.

The transactions which are identified as suspicious are evaluated and examined, after which, if there are doubts as to the legitimate origin of the funds, the necessary reporting to the Money Laundering Compliance Officer and/ or MOKAS takes place. The Company assures the existence of effective communication procedures achieving the timely identification of the unusual and suspicious transactions and their reporting in accordance with the provisions of Applicable Legislation.

Monitoring of accounts and transactions is carried out by the AMLCO in relation to specific types of transactions and economic profile, as well as by comparing periodically the actual movement of the account with the expected turnover as declared at the establishment of the business relationship. Furthermore, the monitoring covers Clients who do not have a contact with the Company as well as dormant accounts showing unexpected movements.

The procedures and intensity of monitoring of accounts and examining transactions are based on the level of applicable risk and, in addition to the detection of unusual or suspicious transactions, must achieve the following:

- Identification of all high-risk clients; the systems or the measures and procedures of the Company are able to produce detailed lists of high-risk clients so as to Facilitate enhanced monitoring of accounts and transactions,
- Investigation of detected unusual or suspicious transactions and, where applicable, relevant internal and external reporting,
- Ascertaining the source and origin of the funds credited to accounts.

All the Company clients' funds are held in separate, segregated accounts that are designated solely for client deposits and withdrawals.

For the deposit to be accepted the Company account holders must have a valid bank or credit card account in their name. The bank/credit card statement must show their name and the same registered address as that shown on their application. The Company matches each deposit to the account name held on file for that customer. As a matter of policy, the Company does

not accept cash or cash equivalents (for example 'travellers' cheques') from Clients.

The withdrawal procedure at the Company follows the strict principle that ensures funds are securely remitted back to their originating source.

The Company reserves the right to refuse to process a transaction where it believes the transaction to be connected in any way to money laundering or criminal activity.

In order to achieve the above purposes, the Company has implemented adequate electronic management information systems which will be capable of supplying the Board of Directors and Money Laundering Compliance Officer, on a timely basis, with all the valid and necessary information for the identification, analysis and effective monitoring of client accounts and transactions based on the assessed risk for money laundering or terrorist financing purposes. These systems may be also used to extract data and information that is missing regarding the client identification and the construction of a client's economic profile.

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 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 the 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 behaviour of employees.

Terrorist Financing:

The funding or 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 – traveller'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 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 non-profit 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.

08 RISK MANAGEMENT AND RISK-BASED APPROACH

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 AMLCO 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.

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 CySEC 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.

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

- Identification, recording and assessment of the money laundering and terrorist financing risks arising from Clients, Financial Instruments, services, and geographical areas of operation of the Company and its Clients.

This function is performed by the Money Laundering Compliance Officer, who is also responsible for determination of the suitable procedures and measures that need to be applied in order to manage such risk,

- Management and mitigation of the assessed risks by the application of appropriate and effective measures, procedures and controls,

- Documenting of the policies, measures, procedures and controls aimed at prevention of money laundering in order to ensure their uniform application within the Company,
- Communication of these policies, measures and procedures to each employee of the Company,
- Continuous monitoring and improvements of the effective operation of the policies, procedures and controls, addressing any possible deficiencies.

The Company monitors and evaluates, on an ongoing basis, the effectiveness of the measures and procedures that have been introduced for the purposes of compliance with applicable Anti- Money laundering legislation.

Risk assessment and implementation of the above measures and procedures result in the categorisation of Clients into the groups of «high-risk» «medium risk» or «low risk» clients. This categorisation is based on criteria which reflect the possible risk causes; each category is accompanied with the relevant due diligence procedures, regular monitoring and controls. Money Laundering Compliance Officer is responsible for preparation and maintenance of the lists for each category of Clients, which include, at least, the Clients' names, account identifications, and dates of commencement of business relationship; these lists are regularly monitored and updated upon the receipt of additional relevant information.

The Company ensures on a continuous basis that the extent of implemented measures and control procedures are proportionate to the risk it faces for the use of services provided, for the purpose of money laundering or terrorist financing.

The measures, procedures and controls for monitoring, evaluation and mitigation of risks are kept under regular review so that risks resulting from changes in the characteristics of existing clients, new clients, services and Financial Instruments are managed and countered effectively on a constant basis.

Specific measures implemented by the Company on a risk-based approach include the following:

- Before the commencement of each new business relationship, in addition to the information relating to the identity of the Client, its addresses, professional and business activities, the prospective client is requested to fill in a separate questionnaire. The validity of the data submitted by the Client represents the criteria which, based on the risk-based approach and of the KYC principles, the Company evaluates and decides on the beginning of cooperation or not. The first contact with the Client and collection of necessary information and data are carried out by the relevant Company's employees, who are responsible for opening the account and beginning a relationship with the Client under supervision of Money Laundering Compliance Officer,
- In order to open an account or perform a transaction, the Company requires from its prospective Clients and Counterparties different sets of documents, depending on the type of business relationship, on legal form of the Client, on whether the Client is a legal or physical person, on whether the Client is subject to supervision by a competent authority of the country of its domicile and other criteria; forms of presentation of KYC and due diligence documents requested by the Company take into account the country of the Clients' domicile or registration,
- The relevant lists of documents and forms of questionnaires to be filled in by the Clients and Counterparties are placed at the official website of the Company; these lists and forms are subject to regular assessment by the Money Laundering Compliance Officer and any necessary amendments to them are introduced, where this is deemed applicable by the Company in order to be compliant with the legislative requirements on a continuous basis and to minimize the possibility of risks relating to the money laundering and terrorist financing activities,
- The Company utilizes information systems, through which the constant monitoring of accounts and transactions is performed, aimed at tracing, monitoring and evaluation of transactions which may be related to the money laundering activities,
- Money Laundering Compliance Officer evaluates on a regular basis the behaviour of client accounts on the basis of the procedures and the criteria of the risk-based approach and, depending on the results, AMLCO draws a decision on whether to continue maintaining these transactions or to consider the termination of business relationship,
- The Company shall not rely on any of the third parties for performance of any of client identification and due diligence procedures; the final responsibility for the certification shall always be borne by the Company itself,
- All the data regarding the identity and transactions of the Client shall be kept by the Company for the period of least five years in accordance with the provisions of Applicable Legislation,
- The Company examines with due diligence every transaction which may, due to its nature, be linked to money laundering and, in case it ascertains the existence of such transactions, it shall follow the necessary procedures provided by Applicable Legislation, including the reporting and investigation procedures,

- In order for the Company's employees to be fully aware of their relevant legal obligations, the Company has established and implemented the employee education and training program, which includes external and in-house trainings, seminars and special programmes. This program aims at educating employees on the latest developments in the prevention of money laundering and terrorist financing, including the practical methods and trends used for this purpose. The training program has 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 is given at regular intervals to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments amendments of legal and/or regulatory requirements, employees' duties as well as any other changes in the financial system of the Republic of Cyprus and/ or other countries and markets.

09 Reporting to MOKAS

All Company employees report to the AMLCO any suspicious transactions or cases where there is an attempt of executing transactions which knows or suspect that are related to money laundering or terrorist financing. The AMLCO is responsible for reporting all the above to MOKAS.

The Company ensures that it maintains adequate information about a Client or its activities to recognize an unusual or suspicious transaction. A list of transactions that might be considered suspicious is included in Appendix C (as described in the Directive).

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

The AMLCO reports to MOKAS suspicious transactions by post, facsimile or by hand.

After the submission of a suspicious report, the AMLCO and the Managing Director decide whether to terminate the relationship with the Client concerned for risk avoidance reasons. In such an event, the Company exercises caution, not to alert the customer concerned that a suspicious report has been submitted to MOKAS. Close liaison with MOKAS is, therefore, maintained to avoid any frustration to the investigations conducted.

After submitting the suspicious report, the Company adheres to any instructions given by MOKAS and, in particular, as to whether or not to continue or suspend a particular transaction or to maintain the particular account active. Furthermore, after the submission of a suspicious report, the customers' accounts concerned as well as any other connected accounts are placed under the close monitoring of the AMLCO.

The Company ensures that in the case of a suspicious transaction investigation by MOKAS, it 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 authorized to manage the account;

d. data of the volume of funds or level of transactions flowing through the account;

e. connected accounts;

f. in relation to specific transactions:
   I. the origin of the funds,
   II. the type and amount of the currency involved in the transaction,
   III. the form in which the funds were placed or withdrawn, for example cash, cheques, wire transfers,
   IV. the identity of the person that gave the order for the transaction,
   V. the destination of the funds,
   VI. the form of instructions and authorization that have been given,
   VII. the type and identifying number of any account involved in the transaction.

ANNEX I

RISK BASED APPROACH – COUNTRIES

(The list may be reviewed)

LOW-RISK COUNTRIES

Member States of the EU

Austria, Estonia, Italy, Portugal, Belgium, Finland, Latvia, Romania, Bulgaria, France, Lithuania, Slovakia, Cyprus, Germany, Luxembourg, Slovenia, Croatia, Greece, Malta, Spain, Czech Republic, Hungary, Netherlands, Sweden, Denmark, Ireland, Poland, United Kingdom

*Gibraltar is a British Overseas Territory within Europe. It is part of the European Union and is directly subject to the requirements of the money laundering directive, which it has implemented. It therefore has the same equivalence status as an EU member state.

The European Economic Area (EEA) EEA-Countries

Iceland, Liechtenstein and Norway

Protocol Territories

Akrotiri and Dhekelia, Channel Island, Faroe Islands, Isle of Man, Jersey, Åland Islands

Countries outside the EU/EEA which are assessed as low-risk countries (Reference is to be made to BASEL AML Index of 2018, countries scored <5.0. In case of a doubt, please further refer to the FATF on the specific country evaluation report)

Australia, Singapore Brazil, Guatemala, New Zealand, Chile, Macedonia, Azerbaijan, Israel, Qatar, Australia, Montenegro, Mauritius, Jordan, St. Lucia, St. Vincent And Grenadines, Colombia, Grenada, Dominica, Chile, Uruguay, South Korea, Canada

MEDIUM-RISK COUNTRIES (BASEL AML Index of 2018, countries scored >5.0<7.0)

Switzerland, Hong-Kong, USA, Saudi Arabia, Qatar, Gambia, Japan, Peru, Taiwan, China, Mexico, Armenia, India, Georgia, Bahrain, South Africa, Egypt, Moldova, El Salvador, Costa Rica, Malaysia, Kuwait, Albania, Venezuela, United Arab Emirates, Indonesia, Bangladesh, Dominican Republic, Uzbekistan, Russia, Bosnia-Herzegovina, Honduras, Marshall Islands, Philippines, Lebanon, Bolivia, China, Ukraine, Turkey, Guyana, Kyrgyzstan, Senegal, Panama, Morocco, Ecuador, Thailand, Timor-Leste (east Timor), Algeria, Kazakhstan, Vanuatu, Jamaica, Angola, Argentina, Cote D'Ivoire, Mongolia, Tanzania, Nicaragua, Paraguay, Nigeria, Zimbabwe

HIGH-RISK COUNTRIES based on:

- ✓ **COMMISSION DELEGATED REGULATION (EU) 2016/1675**
- ✓ **COMMISSION DELEGATED REGULATION (EU) 2018/105**
- ✓ **COMMISSION DELEGATED REGULATION (EU) 2018/212**

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

1	Afghanistan
2	Bosnia and Herzegovina
3	Guyana
4	Iraq
5	Lao PDR
6	Syria
7	Uganda
8	Vanuatu
9	Yemen
10	Ethiopia
11	Sri Lanka
12	Trinidad and Tobago
13	Tunisia
14	Pakistan

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

1	Iran

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

1	Democratic People's Republic of Korea (DPRK)

HIGH-RISK COUNTRIES (BASEL AML Index of 2018, countries scored >7.0)

Cape Verde, Sierra Leone, Benin, Haiti, Vietnam, Kenya, Liberia, Myanmar, Guinea-Bissau, Laos, Afghanistan, Mozambique, Tajikistan

VERY HIGH-RISK COUNTRIES (internal classification)

Iran, North Korea

THE FOLLOWING COUNTRIES ARE EXCLUDED FROM OUR SERVICES

USA, Syria, Sudan, Cuba, British Columbia, Canada, Myanmar, Japan

ANNEX II

INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

INFORMER'S DETAILS		
Name:		Tel:
Department:		Fax:
Position:		
CUSTOMER'S DETAILS		
Account number(s):		
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 MOKAS: Yes/No	Date Reported:	Ref.

ANNEX III

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**

ANNEX IV

COMPLIANCE OFFICER'S REPORT TO MOKAS

COMPLIANCE OFFICER'S REPORT TO MOKAS		
General Information		
Company's Name		
Address where customers account is kept		
Date when business relationship established		
Type of account/s and number/s		
Details of natural person/s and/or legal entities involved in the suspicious transaction/s		
Natural Persons	**Beneficial owner/s of account/s**	**Authorised signatories of the account/s**
Name/s		
Residential Addresses		
Business Address		
Occupation and Employer		
Date and place of birth		
Nationality and passport number		
Legal Entities		
Legal entities name, country and date of incorporation		
Business Address		
Main Activities		

		Name/s	Nationality and Passport #	Date of Birth	Residential Address	Occupation and Employers details
Registered Shareholder/s	1 2 3					
Beneficial Owner/s (if different from above)	1 2 3					
Directors	1 2 3					
Authorised signatories of the account	1 2 3					

Details of Suspicious Activities
Details of suspicious activities should be given

1.

2.

ANNEX V

EMPLOYEE ACKNOWLEDGEMENT

All employees share responsibility for behaving in a manner that will enhance the reputation of NBH Markets EU Limited (ex FIDELISCM (CYPRUS) LTD). The firm requests and requires that all employees make a personal commitment to the observation of the highest ethical standards and exercise of proper judgement in all aspects of his/her business dealings.

I, _____, have read the NBH Markets EU Limited (ex FIDELISCM (CYPRUS) LTD) Ltd Anti-Money Laundering Manual. I understand it and agree that I am in compliance and will continue to apply the rules and procedures set forth therein and my obligations thereunder. I agree that throughout the period of my employment with NBH Markets EU Limited (ex FIDELISCM (CYPRUS) LTD). I will comply in each and every respect with the rules and regulations and all other laws with respect to the prevention of money laundering and terrorist financing.

Date: ___ / ___ / _____

Job Title / Function: _____

Employees signature: _____

ANNEX VI

SOURCE OF WEALTH AND FUNDS

Request of proof of Source of wealth is an additional due diligence measure which is applied to customer profiles on a risk-based approach.

For all deposits Funding Department uploads information to internal system about incoming transaction whether the deposit has been transferred from EU/Non-EU Bank of through Payment System.

Medium Risk Clients

Deposit within PSP over 15K EUR (or equivalent) - to ask client to provide confirmation of Source of Income.

Within non-EU Bank over 30K EUR (or equivalent) – to prove with the client the source of funds by e-mail.

Within non-EU Bank over 50K EUR (or equivalent) - to ask client to provide confirmation of Source of Income.

Within EU Bank over 100K EUR (or equivalent) - to check bank swift and to prove with the client the source of funds by e-mail.

Within EU Bank over 200K EUR (or equivalent) - to ask client to provide confirmation of Source of Income.

**applies to clients whose bank and residence are in same country. Otherwise limits of high-risk clients to be applied.*

High Risk Clients

Deposit within PSP over 15K EUR (or equivalent) - to ask client to provide confirmation of Source of Income.

Within non-EU Bank over 15K EUR (or equivalent) – to prove with the client the source of funds by e-mail.

Within non-EU Bank over 30K EUR (or equivalent) - to ask client to provide confirmation of Source of Income.

Within EU Bank over 50K EUR (or equivalent) – to check bank swift and to prove with the client the source of funds by e-mail.

Within EU Bank over 100K EUR (or equivalent) - to ask client to provide confirmation of Source of Income.

**EU Banks means banks based in EU, EEA and Switzerland.*

The general rule to request from the client to provide confirmation of Source of Income is the following:

To check the nature of income from the questionnaire, to check the deposit transaction(s) and after to choose from list below types of documents to request from the client.

Documents to be uploaded to CRM must be legible and clearly show, that the investment funds belong to the relevant client.

List of examples of information and/or supporting documentation to establish Source of Wealth and Funds:

**Information means data to be collected from questionnaire and provided documents from the client. If missing – to ask the client to provide/explain.*

Source of Funds/Wealth	Information* / Documents that may be Required
Employment Income	**Information:** - Nature of employer's business - Name and address of the employer **Documents:** - Annual salary and bonuses for the last couple of years *OR* - Last month/recent pay slip *OR* - Confirmation from the employer of annual salary *OR* - Bank Statement showing receipt of salary *OR* - Latest accounts or tax declaration if self employed.
Savings / Deposits / Investments	**Information:** - Description of the source of wealth (if no in questionnaire) **Documents:** - Statement from the Bank account/ Depositary/ Trading account/ Portfolio management account/ alternative pension statement etc.

Property Sale	**Information:** - Details of the property sold (i.e. address, date of sale, sale value of property sold, parties involved) **Documents:** - Copy of contract of sale OR - Title deed from land registry and bank statement showing incoming balance transaction from sale
Sale of shares or other investment	**Information:** - Date of sale - Sale value of shares sold and how they were sold (i.e. name of stock exchange) **Documents:** - Copy of contract OR - Statement of account from agent OR - Transaction receipt/confirmation OR - Shareholder's certificate.
Loan / Borrowings	**Information:** - Amount, date and purpose of loan - Name and address of Lender - Details of any security **Documents:** - Loan agreement
Company Sale	**Information:** - Total sales price - Name and Address of Company - Nature of business - Date of sale and receipt of funds **Documents:** - Copy of the contract of sale AND one of: - Internet research of Company Registry OR - Clients' share participation OR - Media coverage.
Company Profits / Dividends	**For Company Profits:** - Copy of latest audited financial statements OR - Copy of latest management accounts - Tax declaration form **For Dividends:** - Board of Directors approval AND - Dividend distribution
Inheritance	**Information:** - Name of deceased - Date of death - Relationship to client - Date received - Total amount - Solicitor's details **Documents:** - Tax clearance documents OR - Lawyer Confirmation
Gift	**Information:** - Date received - Total amount - Relationship to client **Documents:** - Letter from donor explaining the reason for the gift and the source of donor's wealth AND - Identification documents of donor AND - Donor's source of wealth.

Maturity/ Surrender of life policy	**Information:** - Amount received - Policy provider - Policy number/reference - Date of surrender
Pension	- Annual Pension Statement
Other income sources	**Information:** - Nature of income - Amount - Date received and from whom **Documents:** - Appropriate supporting documentation

ANNEX VII

RISK ASSESSMENT PROCEDURE

Risk management is a continuous process, carried out on a dynamic basis. The check of active clients should be done at least twice a year for "high risk" clients and yearly for "medium risk" clients by AMLCO of the Company. Additional check can be made according to the internal decision. Monitoring of transactions of client's funds held in cooperation with Safeguarding Funds Officer.

Additional measure for Risk Assessment Monitoring of existing clients is carrying out as follows:

- Clients under PEP category are checked quarterly
- In case the existing client applies for additional account (the reason should be provided)
- In case the existing client applied for Portfolio Management service, the suitability test is required, and it must be approved by the Head of Portfolio Management to provide a suitable strategy for this specific client. Additionally, the profile of this client will be checked by Back-office (On-boarding).

The extend the Risk based approach the Company through its AMLCO is conducting regular assessment of risks presented by clients from AML perspective. For assessment the following criteria about clients are chosen for objective evaluation:

1. If the client categorized as PEP
2. Country of Domicile (considering Basel Index Score)
3. If the client is face-to-face or non-face-to -face
4. Existence of several accounts in one currency (for self-traders only)
5. Size of Investment
6. Type of services requested (self-trader of Portfolio Management service)
7. Client's bank account (EEA/ Third country/ PSP)

For Existing clients, additional information might be considered:

- Frequency of client's balance transaction
- Change of status of the client (i.e. company is not active any more etc.)
- Changes of knowledges and experience of the client
- World Check status of the client change
- Change of country of residence of the client
- Trading volume of the client
- Any other information found about the client in other sources which may require check.

ANNEX VIII

INTERNAL STATUSES OF ACCOUNTS AND CLIENTS' PROFILES

TRADING ACCOUNTS STATUSES:

Inactive - account has no activity whatsoever (no trades/ transactions). This is account that has been opened for the new client (profile is verified). If for 2 months there were no deposit - the automatic e-mail has to be sent to the client giving one more month to deposit the account:

"Dear Client,
please note that your trading account number…. has been inactive for 2 months. You have one month as from date of this e-mail to activate your account. Otherwise your account will be automatically archived.
This does not affect your profile and other accounts.
In case you have any questions kindly contact compliance@nbhm.eu

If the client does not reply or is not interested to proceed with the deposit - after one month from e-mail the On-boarding change status to "**cancelled**" and it should be "disabled" in MT4 and "archived-YES".

Active - account has at least 1 trade or balance transaction for the last 3 months.

Dormant_1_year - account had activity in the past but does not have any activity for the last 1 year and more.

*A daily fee, which represents an Administrative Fee equal to USD …(….United States Dollars) shall be deducted from the Dormant Account as from the fourth month onwards and then on a continuous daily basis provided (only in case when client does not have other active account).

The e-mail must be sent to notify the client about dormant fee charge to be applied.

When **dormant** account has balance zero – automatically CRM change their status to "**Closed**" and archive. It should be "disabled" in MT4 by Execution.

Cancelled - new accounts without deposits and trades for 2 months (+ 1 month after contacting the client).

Closed - account that was closed:

- according to the request of the clients
- compulsory closed (due to manipulation on the account etc.)
- if the account had no deposit or trading activity for 3 months
- dormant account that became zero balance

PROSPECTIVE AND EXISTING CLIENTS' PROFILES STATUSES

PROSPECTIVE CLIENTS' PROFILES STATUSES:

New - this are non-completed profiles due to missing of documents/ non-completed questionnaire/ missing information/ missing poof of income/ suitability or appropriateness test is not passed/ etc. Shouldn't be treated as clients as they never got services from the company.

If 2 months passed from the moment of registering of profile, the e-mail has to be sent to client stating about giving one more month to complete profile.

If no reply from the client – to cancel the profile and to delete.

Inactive - this are registered and verified profiles but without any activity (balance or trading). Shouldn't be treated as clients as they never got services from the company.

If 2 months passed from the moment of final completion of the profile and no deposit - the e-mail has to be sent to client stating about giving one more month to complete profile.

If no reply from the client – to cancel the profile and to delete.

Cancelled – status related to clients' profiles meaning that during 3 months the profiles haven't been completed (verified) or after the verification for 3 months there were no deposit to trading account or the client made a request to close (cancel) his profile application. For **cancelled** profiles, the log in to the client area must be disabled and all data deleted.
***the time for completion of profile can be expanded based on individual case of the client and/or as per management approval.**

EXISTING CLIENTS' PROFILES STATUSES:

Status of profile of the client is based on activity of all client's accounts.

1. **Dormant_1_year** - client had activity in the past but does not have any activity for the last 1 year and more. *To notify the client that the Company cannot keep funds without service provision and according to no activity to withdraw funds back. If the client replies that he is going to trade – to ask to profile if necessary.*
2. **Dormant_6_months** - account had activity in the past but does not have any activity for the last 6-12 months.
3. **Dormant_3_months** - account had activity in the past but does not have any activity for the last 3-6 months. *To notify the client by email that the status of his profile became "Dormant".*
4. **Active** - has at least one active account at least 1 trade or balance transaction for the last 3 months.
5. **Closed** – ID profile of the client that has changed status due to the direct request of the client or compulsory closed (due to move of accounts under another ID profile etc.), or when all dormant accounts are zero balance.

Balance of all accounts should be zero, status of client's accounts in MT4 must be "disabled". In CRM should have statuses "Closed" and "Archived – "YES".

The data related to client's profile and activity is stored up to 7 (seven) years.

ADDITIONAL STATUSES

Archived - is an additional account status in CRM stated as "Archived – "Yes" or "No". These are dormant Accounts with zero balances, closed accounts. Status of Archived accounts must be Closed.

Test - accounts for test purposes created under test profile.

"Under Special Control" - additional status for existing profiles that used by Compliance when special attention is given to the client.

ANNEX IX

FATF Risk-based Approach Guidance for the Securities Sector (updated October 2018)

Final Guidelines on EDD Factors (Geographic Factors)
Combination of the following factors can lead to High-Risk Classification and the need for EDD:

- Customer is sanctioned by the relevant national competent authority for non-compliance with the applicable AML/CFT.
- Customer is a PEP or customer's family members or close associates are PEPs (including where a beneficial owner of a customer is a PEP)
- Customer resides in or whose primary source of income originates from high-risk jurisdictions.
- Customer resides in countries considered to be uncooperative in providing beneficial ownership information
- Customer acts on behalf of a third party and is either unwilling or unable to provide consistent information and complete documentation
- Customer has been mentioned in negative news reports from credible media, particularly those related to predicate offences for ML/TF or to financial crimes.
- Customer's transactions indicate a potential connection with criminal involvement, typologies or red flags as classified by FATF reports.
- Customer is also a securities provider, acting as an intermediary or otherwise, but is either unregulated or regulated in a jurisdiction with weak AML/CFT oversight (example: some third countries; offshore jurisdictions).
- Customer is engaged in, or derives wealth or revenues from, a high-risk cash-intensive business.
- The number of Suspicious Transaction Reports and their potential concentration on particular client groups.
- Customer is a legal entity predominantly incorporated in the form of bearer shares.
- Customer is a legal entity whose ownership structure is unduly complex
- Customers who have sanction exposure (e.g. have business/ activities/ transactions).
- Customer has a non-transparent ownership structure

Final Guidelines on EDD Factors (Geographic Factors)

- Limiting the extent, type or timing of CDD measures
- Obtaining fewer pieces of customer identification data
- Altering the type of verification carried out on customer's identity
- Inferring the purpose and nature of the transactions or business relationship established based on the type of transaction carried out or the relationship established, without collecting additional information or carrying out additional measures related to understanding the nature and purpose
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if transaction or account values rise above a defined monetary threshold) .
- Reducing the frequency of customer identification updates if the securities provider implements or is required to implement a periodic review process based on a formal cycle
- Reducing the degree and extent of on-going monitoring and scrutiny of transactions, for example based on a reasonable monetary threshold

Final Guidelines Product/Customer Transactions suspicious activity indicators:

- Transactions do not have apparent economic rationale.
- Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/reporting thresholds.
- A concentration ratio of transactions relating to a particular and/or higher risk jurisdiction that is notably higher than what is to be expected considering its normal patterns of trading of a customer.
- Frequent trades resulting in losses for which the customer appears to have no concern.
- Sudden spike in transaction volumes, which deviates from previous transactional activity absent any commercial rationale or related corporate action event.
- Mirror trades or transactions involving securities used for currency conversion for illegitimate or no apparent business purposes.
- A pattern of securities transactions indicating the customer is using securities trades to engage in currency conversion. Examples of securities that can be used in this manner include dual-currency bonds, American Depositary Receipts (ADRs) and foreign ordinary shares traded in the Over-the-Counter Market.
- Securities transactions are unwound before maturity, absent volatile market conditions or other logical or apparent reason.

- Trading or journaling in the same security or securities between numerous accounts controlled by the same people (e.g. potential wash sales and/or directed trading).
- Two or more unrelated accounts at the securities firm trade an illiquid or low priced security suddenly and simultaneously
- Purchase of a security does not correspond to the customer's investment profile or history of transactions (e.g. the customer may never have invested in equity securities or may have never invested in a given industry) and there is no reasonable business explanation for the change.
- Transactions that suggest the customer is acting on behalf of third parties with no apparent business or lawful purpose.
- Funds deposited for purchase of a long-term investment followed shortly by a customer request to liquidate the position and transfer the proceeds out of the account.
- Final Guidelines Suspicious Trading or Market Manipulation
- Making a large purchase or sale of a security, or option on a security, shortly before news or a significant announcement is issued that affects the price of the security, which may be suggestive of potential insider trading or market manipulation.
- A request is made to execute and/or clear a buy order and sell order for the same security or similar or correlated securities (and/or on behalf of the same beneficial owner), in close chronology.
- Accumulation of stock in small increments throughout the trading day to increase price.
- Engaging in prearranged or other non-competitive securities trading, including wash or cross trades of illiquid or low-priced securities.
- Marking the closing price of a security.
- Front-running suspected with regard to other pending customer orders.

Final Guidelines Suspicious Movement of funds or securities

- The securities account is used for payments or outgoing wire transfers with little or no securities activities
- Funds are transferred to financial or depository institutions other than those from where the funds were initially received, specifically when different countries are involved.
- Customer "structures" deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.
- Customer engages in excessive journal entries of funds or securities between related or unrelated accounts without any apparent business purpose.
- Payment by third party check or money transfer from a source that has no apparent connection to the customer.
- Customer uses a personal/individual account for business purposes.
- Payment to a third party to which the customer has no apparent connection.
- Frequent transactions involving round or whole dollar amounts.
- The customer requests that certain payments be routed through *nostro or correspondent accounts held by the financial intermediary instead of its own accounts.
- Funds transferred into an account that are subsequently transferred out of the account in the same or nearly the same amounts, especially when origin and destination locations are high-risk jurisdictions.
- A dormant account suddenly becomes active without a plausible explanation (e.g. large amounts are suddenly wired out).
- Frequent domestic and international automated teller or cash machine activity out of character with the customer's expected activity.
- Many small, incoming wire transfers or deposits made using checks and money orders that are almost immediately withdrawn or wired out in a manner inconsistent with the customer's business or history. This may be an indicator of, for example, a Ponzi scheme.
- Wire transfer activity, when viewed over a period of time, reveal suspicious or unusual patterns.
- Transfers of funds or securities are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
- Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.
- Customer transfers/receives funds to/from persons involved in criminal or suspicious activities (as per the information available).
- In/out transactions for substantial amounts on a short-term basis.
- Receipt of unexplained amounts, followed, shortly thereafter, by a request to return amounts.
- Frequent transfers of securities' ownership.
- Use of bearer securities with physical delivery.

- Frequent change of bank account details or information for redemption proceeds, in particular when followed by redemption requests.
- The usage of brokerage accounts as long term depository accounts for funds.

Final Guidelines on EDD - Non Exhaustive List of Mitigation Techniques

- Obtaining additional customer information, such as the customer's reputation and background.
- Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the customer risk profile
- Carrying out additional searches focused on financial crime risk indicator (i.e. negative news screening) to better assess the customer risk profile
- Obtaining additional or more particular information about the intermediary's underlying customer base and its AML/CFT controls
- Undertaking further verification procedures on the customer or beneficial owner if they may be involved in criminal activity.
- Obtaining additional information about the customer's source of wealth or the source of funds involved in the transaction.
- Verifying the source of funds or wealth involved in the transaction or business relationship
- Evaluating the information provided with regard to the destination of funds and the reasons for the transaction
- Seeking and verifying additional information from the customer about the purpose and intended nature of the transaction or the business relationship.
- Requiring that the withdrawal payment is made through the initial account used for investment.
- Increasing the frequency and intensity of transaction monitoring