



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



1. WHAT IS MONEY LAUNDERING?

1.1. Definition

Money laundering is a process of concealing the true origin and ownership of illegally obtained money. Principally, it is proceeds of criminal activities such as illicit drugs, corruption, organized crime, fraud, sex trade, forgery, illegal logging/fishing, revenue evasion, counterfeit money, piracy, terrorism etc. which criminals attempt to disguise.

1.2. Money Laundering process

There is more than one method of laundering money. Methods can range from purchase and resale of real estate or a luxury item to passing money through a complex web of legitimate businesses and 'shell' companies. In most cases, the proceeds of these criminal activities take the form of cash. There are three stages of money laundering, during which there may be numerous transactions made by launderers that could alert us.

1.3. Placement

Placement is the physical disposal of the cash or asset derived from illegal activity. It includes the opening of numerous bank accounts, depositing cash, and using cash to purchase high value goods such as property, art, jewellery or businesses.

1.4. Layering

Layering is the separation of criminal proceeds from their source by creating complex layering process of financial transactions designed to defeat that audit trail and provide anonymity. It may include telegraphically transferring funds overseas, depositing cash overseas, reselling goods previously with cash.

1.5. Integration

Integration provides apparent legitimacy to criminally derived wealth. If the layering process succeeds, integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds. This may be achieved through a complex web of transfers or income from apparently legitimate businesses previously purchased with the proceeds of illegal activities.

2. WHAT IS FINANCING OF TERRORISM?

Terrorist financing involves collecting and providing funds for terrorist activity. The primary objective of terrorism is to 'to intimidate a population, or to compel a Government or an international organization to do or abstain from doing any act'. The goal of the terrorist or terrorist organization is to maintain financial support in order to achieve their aims, and a successful terrorist group, is one that is able to build and maintain an effective financial infrastructure.

Terrorist need finance for a wide variety of purpose – recruitment, training, travel, materials, and setting up safe havens.

Terrorist control funds from a variety of sources around the world and employ sophisticated techniques to move funds between jurisdictions. In order not to be detected, a terrorist group draws in the service of banks and non-banking institutions and takes advantage of their services products.



3. GENERAL POLICY

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

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

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

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

Such measures include:

- identifying and assessing the Money Laundering and Terrorist Financing risks emanating from particular Clients or types of Clients, financial instruments, services, and geographical areas of operation of its Clients
- managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls
- continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

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

Such indicators include the following:

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



- the nature of business transactions.

4. IDENTIFICATION OF RISKS

4.1 General/Principles

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 the use of the Investment and Ancillary Services 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 such procedures which are able to focus on those Clients who fall outside the 'norm'.

The Company shall be, at all times, in a position to demonstrate to the relevant authorities that the extent of measures and control procedures it applies are proportionate to the risk it faces for the use of the Investment Services, for the purpose of Money Laundering and Terrorist Financing.

4.2 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.

5. PROCEDURES TO MANAGE AND MITIGATE RISKS

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

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

6. RELEVANT INTERNATIONAL ORGANISATIONS

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

- (a) FATF - www.fatf-gafi.org
- (b) The UN Security Council Sanctions Committees- www.un.org/sc/committees
- (c) The International Money Laundering Information Network (IMOLIN) - www.imolin.org
- (d) The International Monetary Fund (IMF) – www.imf.org

7. CLIENT ACCEPTANCE POLICY

The Client Acceptance Policy (hereinafter, the "CAP"), following the principles and guidelines described in this Manual, defines the criteria for accepting new Clients



and defines the Client categorisation criteria which shall be followed by the Company and especially by the employees which shall be involved in the Client Account Opening process.

7.1 General Principles of the CAP

The General Principles of the CAP are the following:

- (a) the Company shall classify Clients into various risk categories and based on the risk perception decide on the acceptance criteria for each category of Client
- (b) where the Client is a prospective Client, an account must be opened only after the relevant pre-account opening due diligence and identification measures and procedures have been conducted, according to the principles and procedures set out in the Manual
- (c) all documents and data described in the Manual must be collected before accepting a new Client
- (d) no account shall be opened in anonymous or fictitious names(s)

8. CRITERIA FOR ACCEPTING NEW CLIENTS

(based on their respective risk)

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

8.1 Low Risk Clients

The Company shall accept Clients who are categorised as low risk Clients as long as the general principles are followed.

Moreover, the Company shall follow the *Simplified Client Identification and Due Diligence Procedures* for low risk Clients, according to this Manual.

8.2 Normal Risk Clients

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

8.3 High Risk Clients

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

9. CLIENTS NOT ACCEPTED

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

- Clients who fail or refuse to submit, the requisite data and information for the verification of his identity and the creation of his economic profile, without adequate justification.



- Shell Banks.

10. CLIENT CATEGORISATION CRITERIA

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

10.1. Low Risk Clients

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

- credit or financial institution covered by the EU Directive or equivalent competent authority.
- credit or financial institution carrying out one or more of the financial business activities as t and which is situated in a country outside the EEA, which:
 - a) in accordance with a decision of the Advisory Authority, imposes requirements equivalent to those laid down by the EU Directive or equivalent competent authority; and
 - b) it is under supervision for compliance with those requirements
- listed companies whose securities are admitted to trading on a Regulated Market in a country of the EEA or in a third country which is subject to disclosure requirements consistent with community legislation
- domestic public authorities of countries of the EEA or equivalent competent authority.

It is provided that further to the cases mentioned above, the Company has to gather sufficient information to establish if the Client qualifies as a low-risk Client.

10.2 Normal Risk Clients

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

- any Client who does not fall under the 'low risk Clients' or 'high risk Clients' categories.

10.3 High Risk Clients

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

- Clients who are not physically present for identification purposes (non-face-to-face Clients)
- Clients whose own shares or those of their parent companies (if any) have been issued in bearer form
- trust accounts



- 'Client accounts' in the name of a third person
- PEPs' accounts
- Clients who are involved in electronic gambling/gaming activities through the internet
- Clients from countries which inadequately apply FATF's recommendations
- Clients included in the leaked documents of Mossack Fonseca (Panama Papers)
- cross-frontier correspondent banking relationships with credit institutions-Clients from third countries
- any other Clients that their nature entail a higher risk of money laundering or terrorist financing
- any other Client determined by the Company itself to be classified as such.

11. CLIENT DUE DILIGENCE AND IDENTIFICATION PROCEDURES

11.1 Cases for the application of Client Identification and Due Diligence Procedures

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

- (a) when establishing a Business Relationship
- (b) when carrying out Occasional Transactions amounting to Euro 15,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked
- (c) when there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction
- (d) when there are doubts about the veracity or adequacy of previously Client identification data.

11.2. Ways of application of Client Identification and Due Diligence Procedures

Client identification procedures and Client due diligence measures shall comprise:

- (a) identifying the Client and verifying the Client's identity on the basis of documents, data or information obtained from a reliable and independent source
- (b) 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 person carrying on in financial or other business 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
- (c) obtaining information on the purpose and intended nature of the business relationship
- (d) conducting on-going 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 person engaged in financial or other business 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.

- (e) Screening clients against databases or third party checks for adverse tax-related news.

11.3 Transactions that Favour Anonymity

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

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

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 shall not proceed with the establishment of the Business Relationship or the execution of the occasional transaction.

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

- I. The construction of the Client's economic profile needs to include/follow the principles below:
 - (a) the Company shall be satisfied that it's dealing with a real person and, for this reason, the Company shall obtain sufficient evidence of identity to verify that the person is who he claims to be. Furthermore, the Company shall verify the identity of the Beneficial Owner(s) of the Clients' accounts. In the cases of legal persons, the Company shall obtain adequate data and information so as to understand the ownership and control structure of the Client. Irrespective of the Client type (e.g. natural or legal person, sole trader or partnership), the Company shall request and obtain sufficient data and information regarding the Client business activities and the expected pattern and level of transactions. However, it is noted that no single form of identification can be fully guaranteed as genuine or representing correct identity and, consequently, the identification process will generally need to be cumulative
 - (b) the verification of the Clients' identification shall be based on reliable data and information issued or obtained from independent and reliable sources, meaning those data, and information that are the most difficult to be amended or obtained illicitly
 - (c) a person's residential and business address will be an essential part of his identity



- (d) the Company will never use the same verification data or information for verifying the Client's identity and verifying its home address
- (e) the data and information that are collected before the establishment of the Business Relationship, with the aim of constructing the Client's economic profile and, as a minimum, shall include the following:
 - the purpose and the reason for requesting the establishment of a Business Relationship
 - the anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments
 - the Client's size of wealth and annual income and the clear description of the main business/professional activities/operations
- (f) the data and information that are used for the construction of the Client-legal person's economic profile shall include, *inter alia*, the following:
 - the name of the company
 - the country of its incorporation
 - the head offices address
 - the names and the identification information of the Beneficial Owners
 - the names and the identification information of the directors
 - the names and the identification information of the authorised signatories
 - financial information
 - the ownership structure of the group that the Client-legal person may be a part of (country of incorporation of the parent company, subsidiary companies and associate companies, main activities and financial information).

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

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

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

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

11.6 Further Obligations for Client Identification and Due Diligence Procedures



- I. In addition to the principles described in Section 11.5 above, the Company shall:
- (a) ensure that the Client identification records remain completely updated with all relevant identification data and information throughout the Business Relationship
 - (b) examine and check, on a regular basis, the validity and adequacy of the Client identification data and information that he maintains, especially those concerning high risk Clients.

12. ON-GOING MONITORING PROCESS

12.1 General

The Company has a full understanding of normal and reasonable account activity of its Clients as well as of their economic profile and has the means of identifying transactions which fall outside the regular pattern of an account's activity or to identify complex or unusual transactions or transactions without obvious economic purpose or clear legitimate reason. Without such knowledge, the Company shall not be able to discharge its legal obligation to identify and report suspicious transactions.

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

12.2 Procedures

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

- (a) the identification of:
 - all high risk Clients, as applicable; the Company shall be able to produce detailed lists of high risk Clients, so as to facilitate enhanced monitoring of accounts and transactions, as deemed necessary
 - transactions which, as of their nature, may be associated with money laundering or terrorist financing
 - unusual or suspicious transactions that are inconsistent with the economic profile of the Client for the purposes of further investigation
 - in case of any unusual or suspicious transactions, the head of the department providing the relevant investment and/or ancillary service or any other person who identified the unusual or suspicious transactions
- (b) further to point (a) above, the investigation of unusual or suspicious transactions the results of the investigations are recorded in a separate memo and kept in the file of the Clients concerned
- (c) the ascertainment of the source and origin of the funds credited to accounts
- (d) the use of appropriate and proportionate IT systems, including:
 - i. adequate automated electronic management information systems which will be capable of supplying the Board of Directors on a timely basis, all the valid and necessary information for the identification, analysis and effective monitoring of Client accounts and transactions based on the assessed risk



for money laundering or terrorist financing purposes, in view of the nature, scale and complexity of the Company's business and the nature and range of the investment services undertaken in the course of that business

- ii. automated electronic management information systems to extract data and information that is missing regarding the Client identification and the construction of a Client's economic profile.
 - iii. for all accounts, automated electronic management information systems to add up the movement of all related accounts on a consolidated basis and detect unusual or suspicious activities and types of transactions. This can be done by setting limits for a particular type, or category of accounts (e.g. high risk accounts) or transactions (e.g. deposits and withdrawals in cash, transactions that do not seem reasonable based on usual business or commercial terms, significant movement of the account incompatible with the size of the account balance), taking into account the economic profile of the Client, the country of his origin, the source of the funds, the type of transaction or other risk factors. The Company shall pay particular attention to transactions exceeding the abovementioned limits, which may indicate that a Client might be involved in unusual or suspicious activities.
- (e) the monitoring of accounts and transactions in relation to specific types of transactions and the 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 exhibiting unexpected movements.

13. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS / ACTIVITIES TO THE UNIT

13.1 Suspicious Transactions

- I. The definition of a suspicious transaction as well as the types of suspicious transactions which may be used for Money Laundering and Terrorist Financing are almost unlimited. A suspicious transaction will often be one which is inconsistent with a Client's known, legitimate business or personal activities or with the normal business of the specific account, or in general with the economic profile that the Company has created for the Client. The Company shall ensure that it maintains adequate information and knows enough about its Clients' activities in order to recognise on time that a transaction or a series of transactions is unusual or suspicious.
- II. Examples of what might constitute suspicious transactions/activities related to Money Laundering and Terrorist Financing are listed in Appendix 3 of the Manual. The relevant list is not exhaustive nor it includes all types of transactions that may be used, nevertheless it can assist the Company and its employees, in recognising the main methods used for Money Laundering and Terrorist Financing. The detection by the Company of any of the transactions contained in the said list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of



the funds, the nature and economic/business purpose of the underlying transaction, and the circumstances surrounding the particular activity.

III. In order to identify suspicious transactions the Company shall perform the following activities:

- monitor on a continuous basis any changes in the Client's financial status, business activities, type of transactions etc.
- monitor on a continuous basis if any Client is engaged in any of the practices described in the list containing examples of what might constitute suspicious transactions/activities related to Money Laundering and Terrorist Financing.

Furthermore, the Company shall ensure the following activities are part of its internal:

- receive and investigate information from the Company's employees, on suspicious transactions which creates the belief or suspicion of money laundering.
- evaluate and check the information received from the employees of the Company, with reference to other available sources of information and the exchanging of information in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors.

15. EMPLOYEES' OBLIGATIONS, EDUCATION AND TRAINING

15.1 Employees' Obligations

- (a) The Company's employees shall be personally liable for failure to report information or suspicion, regarding money laundering or terrorist financing
- (b) the employees must cooperate and report, without delay anything that comes to their attention in relation to transactions for which there is a slight suspicion that are related to money laundering or terrorist financing.

15.2. Education and Training

15.2.1 Employees' Education and Training Policy

- (a) The Company shall ensure that its employees are fully aware of their legal obligations according to the relevant laws, 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.
- (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.

16. INVESTIGATION

Upon notification to the Compliance Officer of any suspicious activity, an investigation will be commenced to determine if a report should be made to appropriate law enforcement or regulatory agencies. The investigation will include, but not necessarily be limited to, review of all available information, such as payment history, birthdates and address.

The Compliance Officer is responsible for any notice or filing with law enforcement or regulatory agency.

Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. Under no circumstances shall any officer, employee or appointed agent disclose or discuss any AML concern, investigation, notice or SAR filing with the person or persons subject of such, or any other person, including members of the officer's/employee's or appointed agent's family. Confidentiality whilst an investigation is on-going is of the utmost importance and employees are reminded of the offence of "tipping off". The Company has the right to terminate the agreement with the Client immediately and to prohibit the client from withdrawing any assets if the explanations provided are inadequate or in conflict with the AML Policy.

17. COMPLIANCE OFFICER

Money Laundering Compliance Officer

17.1 Roles and Responsibilities

The Compliance officer will be responsible for:-

- (a) Creating and keeping this manual current;
- (b) Monitoring the compliance by our business with the requirements of the laws and regulations that relate to AML & CTF;
- (c) Monitoring transactions undertaken for Customers;
- (d) Identification and management of Money Laundering risk using our services
- (e) Providing leadership and training on AML & CTF issues to our staff, including new staff;
- (f) Investigating unusual matters and reporting those that are suspicious to this Manual;
- (g) Monitoring employees in the course of performance of their duties;
- (h) Ensuring that our staffs are aware of the requirements of this manual and of the relevant laws and regulations that apply to our business; and
- (i) Reviewing this manual periodically for its adequacy.