

# **TURNKEY INSURANCE AND REINSURANCE BROKERS LTD**

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

MAY 2019 V.1

# CONTENTS

<b>1.</b>	<b>Introduction .....</b>	<b>3</b>
1.1	Definition of Money Laundering .....	3
1.2	Stages for Money Laundering .....	4
1.3	Definition of Terrorism Financing .....	4
1.4	Money Laundering Offences (Article 4 of the Law) .....	4
1.5	Predicate offences (Article 5 of the Law) .....	5
1.6	Responsibilities.....	5
1.7	Internal Control Systems.....	6
<b>2.</b>	<b>Board of Directors: duties and responsibilities.....</b>	<b>7</b>
<b>3.</b>	<b>Money Laundering Compliance Officer (MLCO) .....</b>	<b>8</b>
<b>4.</b>	<b>Customer Identification and due Diligence Procedures .....</b>	<b>10</b>
4.1	Know your Client Principle (KYC) .....	10
4.2	Clients' Acceptance Procedure .....	10
4.3	Due Diligence and identification data updating of existing Clients.....	11
4.4	Client Categorization.....	11
4.5	Cash Transactions.....	11
4.6	Money transfers to third parties.....	11
<b>5.</b>	<b>Risk Based Approach .....</b>	<b>12</b>
5.1	List of Potential Risks .....	12
5.2	Policies, Procedures and Controls for Risk Containment.....	13
<b>6.</b>	<b>Record Keeping .....</b>	<b>14</b>
6.1	General.....	14
6.2	Format of Records .....	14
6.3	Certification and Language of documents .....	14
6.4	Updating of Clients Identification Records .....	14
<b>7.</b>	<b>Recognition and Reporting Suspicious Transactions.....</b>	<b>15</b>
7.1	Employee's Obligations.....	15
7.2	How to Identify a Suspicious Transaction .....	15
7.3	Reporting of Suspicious Transactions Internally and to the Authorities .....	16
<b>8.</b>	<b>Education and Training of Staff .....</b>	<b>17</b>
	Acronyms .....	18
	APPENDIX 1: KYC Form .....	19
	APPENDIX 2: Internal Suspicion Report for Money Laundering and Terrorist Financing .....	23
	APPENDIX 3: Internal Evaluation Report for Money Laundering and Terrorist Financing .....	24
	APPENDIX 4: Examples of Suspicious Transactions/Activities Related to Money Laundering and Terrorist Financing .....	25

# 1. Introduction

The Prevention and Suppression of Money Laundering Activities Law of 2007, N.188(I)/2007, as amended (the "**Law**") recognizes the important role of the financial sector for the forestalling and effective prevention of money laundering and terrorist financing activities and places additional administrative requirements on all financial institutions.

The Law requires all persons carrying on financial and other business to establish and maintain specific policies and procedures to guard against their business and the financial system in general being used for the purposes of money laundering. These procedures are designed to achieve two main purposes:

- a) To facilitate the recognition and reporting of suspicious transactions
- b) To ensure through the strict implementation of the "know-your-customer" principle and the maintenance of adequate record keeping procedures, should a customer come under investigation, that the financial institution is able to provide its part of the audit trail.

The Risk Management and Procedures Manual for the Prevention of Money Laundering and Terrorist Financing (hereafter refers as the "**Manual**") provides the guidelines that should be followed throughout the Company to assist in the detection and/or prevention of moneylaundering and terrorist financing activities in accordance with the Law and the relevant Directive 144-2007-08 of the Cyprus Securities and Exchange Commission ("**CySec**"), or any other Directive or Circular amending, substituting or supplementing the said Directive 1442007-08.

The aim of this Manual is to provide the guidelines that should be followed throughout **Turnkey Insurance and Reinsurance Brokers Ltd** (hereafter refers as the "**Company**") for the detection and/or prevention of money-laundering activities and terrorist financing. All Company's staff shall perform their duties as per the guidelines set out in this Manual and the relevant Company Operations Manuals.

## 1.1 Definition of Money Laundering

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

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

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

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

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

## 1.2 Stages for Money Laundering

There is no single method of laundering money. Despite the variety of methods employed, the laundering process is accomplished in three basic stages which may comprise transactions by the

launderers that could alert a financial institution to criminal activity:

- > **Placement** - The process of placing, through deposits or other means, unlawful cash proceeds into traditional financial institutions.
- > **Layering** - The process of separating the proceeds of criminal activity from their origin through the use of layers of complex financial transactions, such as converting cash into traveler's cheques, money orders, wire transfers, letters of credit, stocks, bonds, or purchasing valuable assets, such as art or jewelry. All these transactions are designed to disguise the audit trail and provide anonymity.
- > **Integration** - The process of using an apparently legitimate transaction to disguise the illicit proceeds, allowing the laundered funds to be disbursed back to the criminal. Different types of financial transactions, such as sham loans or false import/export invoices, can be used. If the layering process is successful, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

The three basic steps may occur as separate and distinct phases or may occur simultaneously or, more commonly, they may overlap. How the basic steps are used depends on the available laundering mechanisms and requirements of the criminal organizations.

### 1.3 Definition of Terrorism Financing

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

Terrorism financing is an offence by any means, directly or indirectly, unlawfully and willfully, which provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in whole or in part, in order to carry out an act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

### 1.4 Money Laundering Offences (Article 4 of the Law)

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

- Converts or transfers or removes such property for the purpose of concealing its illicit origin or of assisting any person who is involved in the commission of a predicate offence to evade the legal consequences of his actions
- Conceals or disguises the true nature, the source, location, disposition, movement, rights with respect to property or ownership of this property;
- Acquires, possesses or uses such property
- Participates in, associates or conspires to commit or attempts to commit and aids and abets and provides counseling or advice for the commission of any of the above mentioned offences
- Provides information with respect to investigations that are being performed for laundering offences for the purpose of enabling the person who acquired a benefit from the commission of a

predicate offence to retain the relevant proceeds

### 1.5 Predicate offences (Article 5 of the Law)

Predicate offences are all criminal offences punishable with imprisonment exceeding one year from which proceeds were generated that may become the subject of a money laundering offence. Proceeds mean any kind of property which has been generated by the commission of a predicate offence. Among others are the following:

- a) drug trafficking
- b) fraud
- c) theft
- d) premeditated and attempted murder
- e) illicit importation, exportation, purchasing, selling disposition, possession, transfer and trafficking of arms and munitions
- f) importation, exportation, purchasing, selling, disposition, possession, transfer of stolen objects, pieces of art, of antiquities and tokens of cultural heritage
- g) detachment of money or of property of any kind by use or threat of use of force or other illicit act
- h) living on the earnings of prostitution and offences associated with procurement and seduction of women and minors
- i) offences relating to corruption of public or private servants

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

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

### 1.6 Responsibilities

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

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

The procedures and recommendation contained in this Manual must be followed strictly by the Company's personnel. Staff should be made aware of the seriousness of Money Laundering and Terrorist Financing activities, their own statutory obligations and be encouraged to co-operate and report suspicious transactions promptly. This can be done through the completion of the Internal Suspicion Report for Money Laundering and Terrorist Financing, which can be found in **Appendix 2**, and should be submitted, to the Money Laundering Compliance Officer ("**MLCO**").

It is the responsibility of all Company employees to read and understand the Company's AntiMoney Laundering and Terrorist Financing Manual.

Each employee receives a copy of the Manual and has to sign that he/she has read and understood its contents and understands the responsibilities and procedures outlined in it.

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

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

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

## **1.7 Internal Control Systems**

Internal Control Systems should be established so as to monitor compliance with the procedures introduced by the Company for the prevention and detection of Money Laundering. The compliance function is responsible to conCompany adherence to various Anti-Money Laundering procedures through specifically designed audits and/or other functional audits.

## **2. Board of Directors: duties and responsibilities**

The Company's Board of Directors shall have the duty to:

- a) determine records and approve the general policy principles of the Company in relation to the prevention of Money Laundering and Terrorist Financing and communicates them to the MLCO.
- b) appoint a MLCO and, where necessary, assistant compliance officers and determines their duties and responsibilities, which are recorded in this manual. The MLCO is part of the management of the Company so as to command the necessary authority.
- c) approve the Anti-Money Laundering and Prevention of Terrorist Financing Manual, which is communicated to all the Company's employees 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.
- d) ensure that all requirements of the Law and the Directive are applied, and to assure that appropriate, effective and sufficient systems and controls are in place.
- e) assure that the MLCO and his/her assistants and any other person who has been assigned the duty of implementing the procedures for the prevention of money laundering and terrorist financing, have complete and timely access to all data and information concerning client 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.
- f) ensure that all employees are aware of the person who has been assigned the duties of the MLCO, as well as his assistants, and to whom they report, any information concerning transactions and activities of which they have knowledge or suspicion might be related to money laundering and/or terrorist financing.
- g) establish a clear and quick reporting chain through which information regarding suspicious transactions is passed without delay to the MLCO.
- h) assess and approve the Annual Anti-Money Laundering and Terrorist Financing Report and to take all action deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the Report.

### 3. Money Laundering Compliance Officer (MLCO)

The MLCO is generally responsible to ensure that the operations and activities of the Company are in compliance with the Law, the Directive, and the general legal and regulatory framework that relate to ML & TF; and to review, appraise and report and monitor relevant action on compliance issues as required. The MLCO reports primarily to the Chairman of the Board of Directors and directly to the BoD.

Due to the principle of Proportionality the MLCO is the CEO of the Company.

The MLCO duties should include at least, the following:

- a) Based on the general policy principles set by the BoD of the Company, the MLCO designs the internal practices, measures, procedures and controls relevant to the prevention of money laundering and terrorist financing, and describes and explicitly allocates the appropriateness and the limits of responsibility of each department that is involved in the abovementioned.
- b) Develops and establishes the clients' acceptance policy and submits it to the BoD for consideration and approval. [KYC – **Appendix 1**]
- c) Monitors and assesses the correct and effective implementation of the policy, and the implementation of the AML Manual. Applies appropriate monitoring mechanisms and, in the event that he identifies shortcomings and/or weaknesses in the application of the set practices, measures, procedures and controls, gives appropriate guidance for corrective measures and where he deems necessary informs the BoD.
- d) Receives information from the Company's employees which is considered to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities. The information is received in a written report form (**see Appendix 2**).
- e) Examines and evaluates the information received as per paragraph (e), by reference to other relevant information and discusses the circumstances of the case with the informer and, where appropriate, with the informer's superiors. The evaluation of the information reported should be recorded and retained on file, (**see Appendix 3**).
- f) If following the evaluation described in paragraph (e), the MLCO decides to notify MOKAS, he completes a report and submits it to MOKAS the soonest possible. After the submission of the MLCO's report to MOKAS, the accounts involved and any other connected accounts, are closely monitored by the MLCO and following any directions from MOKAS, thoroughly investigates and examines all the transactions of the accounts.
- g) If following the evaluation described in paragraph (e) the MLCO decides not to notify MOKAS, then he fully explains the reasons for such a decision in the "Internal Evaluation Report".
- h) Acts as the first point of contact with MOKAS, upon commencement and during an investigation as a result of filing a report to MOKAS.
- i) Responds to all requests and queries from MOKAS, provides all requested information and fully cooperates with MOKAS.
- j) Ensures the preparation and maintenance of the lists of clients recording money laundering risk profiles.
- k) Ensures that any branches and subsidiaries of the Company that may operate in countries outside the European Economic Area, have taken all necessary measures for achieving full compliance with the provisions of the present Directive, in relation to client identification, due diligence and record keeping procedures.



- l) Provides advice and guidance to the employees of the Company on subjects related to money laundering and terrorist financing.
- m) Acquires the required knowledge and skills for the improvement of the appropriate procedures for recognising, preventing and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing.
- n) Determines the Company's departments and employees that need further training and education for the purpose of preventing money laundering and terrorist financing and organises appropriate training sessions/seminars. Assesses the adequacy of the education and training provided.
- o) Prepares if required by the BoD a Report and submits it to the BoD for approval.
- p) Maintains a registry which includes the reports of points (d), (e) and (f), and relevant statistical information (department that submitted the internal report, date of submission to the MLCO, date of assessment, date of reporting to MOKAS), the evaluation reports of point (c) and all the documents that verify the fulfillment of his duties specified in the present subparagraph.
- q) During the execution of his duties the MLCO obtains and utilizes data, information and reports issued by relevant international organizations.

## **4. Customer Identification and due Diligence Procedures**

It is required that the Company maintains certain identification procedures to verify its customers' identity. The identity of a prospective customer should be established at the time of establishing an account relationship and prior to the execution of any transaction or the provision of any services whatsoever. The execution of any transaction or the provision of any services prior to establishing the identity of the customer is strictly prohibited. This is done through a KYC Form (Appendix 1).

Every reasonable effort should be made to determine the true identity of any person who asks to open an account, enters into a business relationship with the Company, or undertakes a significant one-off transaction or a series of linked transactions.

### **4.1 Know your Client Principle (KYC) – Appendix 1**

"Know Your Client" processes are intended to enable the Company to form a reasonable belief that it knows the true identity of each customer before the client enters into a business relationship with the Company.

The need to effectively KYC is at the very heart of an efficient anti-money laundering management system. KYC due diligence is a continuous process and not only limited to clients seeking to open new business opportunities. While client identification procedures are aimed at establishing clients' identity, the Company is also required to decide whether the clients' risk-profile necessitates enhanced due diligence procedures.

The resources used to undertake effective customer due diligence are not prescribed. Various sources may be used to enhance a business' knowledge of its client, including direct discussion with the client, information (e.g. websites, brochures, reports etc) prepared by the client and review of public domain information.

### **4.2 Clients' Acceptance Procedure**

Generally, prior to the establishment of a business relationship the following procedures must be performed:

- (1) Every potential new client of the Company has to complete KYC (specimen in Appendix 1) forms and return them along with the supporting documents required if any.
- (2) Identify the client and verify the client's identity on the basis of data, documents or information obtained from reliable and independent sources.
- (3) In case the client - legal entity identify the beneficial owner and take adequate measures to verify his identity based on records, documents or information obtained from independent and reliable sources.
- (4) Identify the clients' Risk Profile. Clients should be designated as high, low or normal risk. For the identification criteria refer to Paragraph 4.4.

### **4.3 Due Diligence and identification data updating of existing Clients**

The client identification data and records should be reviewed on a regular basis or whenever there are doubts for their accuracy. In addition to the above cases, the Client's identity and business/economic profile should be checked in case any of the following occurs:

- i. There is a material change in the customer's legal status such as:
  - a) Change of beneficial owners
  - b) Change of trustee
  - c) Change of corporate name/trading name used

If a Client fails or refuses to submit, within a reasonable timeframe, the required data and identification information for the updating of his/her identity and business/economic profile and, as a consequence, the Company is unable to comply with the customer identification requirements set out in the Law and the Directive, then the Company will consider the possibility to terminate the business relationship and inactivate or close all services provided, while at the same time it should examine whether it is warranted under the circumstances to submit a report of suspicious transactions/activities to MOKAS.

### **4.4 Client Categorization**

The Company should assess whether the particular Client poses a risk of money laundering and on basis of such assessment Clients should be categorized as "high", "low" or "normal risk".

The category of each client should be maintained in the Company's records, and which must also contain the following information: clients name, account number, and date of commencement of business relationship.

### **4.5 Cash Transactions**

Generally Clients' will have to deposit their funds directly into the Company's client accounts or directly to the Insurance / Reinsurance Undertaking. The Company may also accept cash from clients up to an amount of €10.000. No amounts above this limit will be accepted.

### **4.6 Money transfers to third parties**

The Accounts Department is not allowed to authorise third party transfers unless the following three conditions are all fulfilled:

- a. there is a written request for a transfer between accounts signed by both the transferor and the transferee;
- b. the BACK OFFICE verifies the signature and conCompanies the client's request, unless the request is signed in the presence of Company staff, and such signature is so witnessed; and
- c. the transaction is approved by the Executive Chairman or the Executive Director (1).

## 5. Risk Based Approach

### 5.1 List of Potential Risks

#### 1. Clients acceptance risk Clients' Behaviour risks

Determining the potential money laundering risks posed by a client will provide significant input into the overall money laundering risk assessment. The Company will assess, whether a particular client poses a higher risk of money laundering and whether mitigating factors may lead to a determination that clients engaged in such activities do not pose a higher risk of money laundering. Application of the risk variables described further below plays an important part in this determination. There is no universal consensus as to which clients pose a higher risk, but the below listed characteristics of clients have been identified with potentially higher money laundering risks:

- Non face-to-face clients
- 'Client accounts' in the name of a third person
- 'Politically exposed persons' accounts
- Companies incorporated in offshore centres,
- Clients from high risk countries or from countries known for high level of corruption or organized crime or drug trafficking
- Clients whose identification is difficult to check

The following factors should also be considered in association with the clients' characteristics and behaviour:

- Unwillingness of clients to provide information on the beneficial owners of a legal person;
- Clients willing to pay unusual fees to have services provided.

#### 2. Country/jurisdiction risks

Country/area risk, in conjunction with other risk factors, provides useful information as to potential ML & TF risks. There is no universally agreed definition by either governments or institutions that prescribes whether a particular country represents a higher risk. Factors that may result in a determination that a country poses a higher risk include:

- Any country subject to trade sanctions embargoes or similar measures issued by, for example, the United Nations ("UN").
- Any country known to be a tax haven, source of narcotics or other significant criminal activity.
- Countries identified by credible sources as providing funding or support for terrorist activities.
- Countries/areas identified by credible sources as having significant levels of corruption, or other criminal activity, including source or transit countries/areas for ongoing criminal activity, such as illegal drugs, human trafficking and smuggling, systematic frauds and illegal gambling.

### 5.2 Policies, Procedures and Controls for Risk Containment

The BoD, with the advice of the MLCO, formulates policies, procedures and controls in response to the Company's particular circumstances and characteristics.

Further to the above policies, the Company shall employ, where needed on a case-by-case basis, the following measures and controls so as to mitigate the potential money laundering and terrorist financing risks presented by those clients that are determined to be of higher risk as the result of the institution's risk assessment process.

- An increased level of due diligence should be applied to those clients determined to be of higher risk.
- Increased awareness by the institution of higher risk situations within business lines across the institution;
- Increased levels of know your client ("KYC") or enhanced due diligence;
- Escalation for approval of the establishment of a relationship;
- Increased levels of ongoing controls and reviews of relationships.

**With respect to transactions or business relationships with Politically Exposed Persons (PEPs), the Company shall:**

The decision for establishing a business relationship with a Politically Exposed Persons is taken by Compliance Department and BoD of the Company. When establishing a business relationship with a client (natural or legal person) and subsequently it is ascertained that the persons involved are or have become PEPs, then an approval is given for continuing the operation of the business relationship by the Chairman or by Executive Director of the Company.

The Company shall obtain adequate documentation to ascertain not only the identity of the said person but also to assess his business reputation (e.g. reference letters from third parties). In more detail the Company shall follow the following procedures when face potential or PEP clients.

- have appropriate identification procedures to determine whether the client is a PEP
- have the Chairman or the Executive Director approval for establishing business relationships with such clients
- conduct ongoing monitoring of the business relationship.

The Company shall apply the above with respect to the PEP's accounts.

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

## **6. Record Keeping**

### **6.1 General**

The Administration/Back-Office Department of the Company shall maintain records of:

- (a) the Client identification documents (KYC and other related documents) obtained during the Client identification and due diligence procedures, as applicable
- (b) the details of all relevant records with respect to the provision of investment services to Clients

The documents/data of mentioned above shall be kept for a period of at least two (2) years, which is calculated after the execution of the transactions or the termination of the Business Relationship.

It is provided that the documents/data mentioned in points (a) and (b) above which may be relevant to ongoing investigations shall be kept by the Company until the investigation has been completed and the case has been closed.

### **6.2 Format of Records**

The Administration/Back-Office Department shall retain the Clients documents/data mentioned in Section 6.1 of the Manual in:

- hard copy form, and/or
- electronic form, provided that the Administration/Back-Office Department shall be able to retrieve the relevant documents/data without undue delay and present them at any time, to the MLCO, after a relevant request.

In case the Company will establish a documents/data retention policy, the MLCO shall ensure that the said policy shall take into consideration the requirements of the Law and the Directive.

### **6.3 Certification and Language of documents**

The documents/data obtained in hard copy, shall be in their original form or in a certified true copy form. The copied documents can be certified as true copies, signed and dated by the employee that obtained the documents.

In case the above documents/information are in a language other than Greek or English, these should be accompanied by a certified true translation.

Each time the Company shall proceed with the acceptance of a new Client, administration staff shall be responsible for ensuring compliance with the provisions of this section.

### **6.4 Updating of Clients Identification Records**

The Back Office must ensure that the client identification records remain updated with all relevant identification data and information throughout the business relationship. The administration staff examines and checks, on a regular basis, the validity and adequacy of the client identification data and information it maintains, especially those concerning high risk clients.

## 7. Recognition and Reporting Suspicious Transactions

### 7.1 Employee's Obligations

- a. The Company's employees can be personally liable for failure to report information or suspicion, regarding money laundering or terrorist financing.
- b. The employees cooperate and report, without delay, anything that comes to their attention in relation to transactions for which there is suspicion that they are related to money laundering or terrorist financing.
- c. The employees fulfill their legal obligation to report their suspicions regarding money laundering and terrorist financing, after they report their suspicions to the MLCO.

### 7.2 How to Identify a Suspicious Transaction

As a general rule, a transaction may be connected to money laundering or terrorist activity financing when it raises questions or gives rise to discomfort, apprehension or mistrust. The context in which a transaction occurs is a significant factor in assessing suspicion. This will vary from business to business and from one client to another.

The reporting person, should evaluate transactions in terms of what seems appropriate and is within normal practices within the Company, and based on the knowledge of the client. The fact that transactions do not appear to be in line with normal industry practices may be a relevant factor for determining whether there are reasonable grounds to suspect that the transactions are related to money laundering or terrorist activity financing.

A single indicator is not necessarily indicative of reasonable grounds to suspect money laundering or terrorist financing activity. However, if a number of indicators are present during a transaction or series of transactions, then a closer look at other factors should be taken prior to making the determination as to whether the transaction must be reported.

The indicators have to be assessed by the MLCO in the context in which the transaction occurs. Each indicator may contribute to a conclusion that there are reasonable grounds to suspect that the transaction is related to the commission of money laundering offence or a terrorist activity financing offence. However, it may also offer no indication of this in view of factors such as the client's occupation, business, financial history and past investment pattern.

Taken together, the presence of one or more indicators as well as knowledge of the client's business or financial affairs may help identify suspicious transactions.

#### General Guidance

Examples of what might constitute suspicious transactions/activities are found in **Appendix 4**. The list is not exhaustive nor does it include all types of transactions that may be used; nevertheless it can assist the employees in recognising the main methods used for money laundering and terrorist financing. The detection of any of the transactions contained in **Appendix 4** 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.

Employees should also report transactions which are thought to be suspicious even if the transactions do not match with the cases described in Appendix 4.

The MLCO needs to decide whether or not an individual transaction is suspicious by comprehensively considering all relevant information at hand.

### **7.3 Reporting of Suspicious Transactions Internally and to the Authorities**

Reports submitted to MOKAS play a major role in combating money laundering, terrorism financing and other major crimes.



## **8. Education and Training of Staff**

The education and training of the Company's personnel on a regular basis is of high importance for the prevention and detection of money laundering and terrorist financing offences. The Company should establish a training program if needed to educate the staff on the latest developments in the prevention of money laundering and terrorist financing.

The following elements will be addressed in the training program:

- The importance BoD and senior management place on ongoing education, training, and compliance.
- Employee accountability for ensuring regulatory compliance.
- Coverage of Company policies, procedures, processes, and rules and regulations.
- Coverage of different forms of money laundering and terrorist financing as it relates to identification and examples of suspicious activity.
- Penalties for noncompliance with internal policies and regulatory requirements
- The Employees' and the Company's responsibilities under the Law, and the consequences of failing to meet them;
- What money laundering and terrorist financing are;
- The Company's procedure for reporting suspicions

In order to be familiarized with the concepts and implications of Money Laundering, all new staff entering the Company will receive the AML Manual (this Manual).

## ACRONYMS

<b>AML</b>	Anti-Money Laundering
<b>AML Manual, the Manual</b>	the Anti-Money Laundering and Prevention of Terrorist (this Manual)
<b>BoD</b>	the Board of Directors of Turnkey
<b>CDD</b>	Client Due Diligence
<b>Company</b>	<b>Turnkey Insurance and Reinsurance Brokers Ltd</b>
<b>Directive</b>	the Directive for the Prevention of Money Laundering and Terrorist Financing - DI144-2007-08
<b>E.E.A.</b>	The European Economic Area - the 27 EU Member States plus Iceland, Liechtenstein and Norway and the U.K.
<b>Executive Director</b>	Luke Benfield
<b>FATF</b>	Financial Action Task Force
<b>Law</b>	the Prevention and Suppression of Money Laundering Activities Law of 2007, N.188 (I)/2007
<b>MLCO</b>	Money Laundering Compliance Officer
<b>ML &amp; TF</b>	Money laundering and Terrorist Financing
<b>MOKAS Report</b>	the Independent Unit for Combating Money Laundering The annual report prepared by the MLCO according to paragraph 10 of the Directive.
<b>Republic</b>	The Republic of Cyprus



STRICTLY CONFIDENTIAL

TURNKEY

<u>S.No.</u>	<u>Particulars</u>	<u>Details</u>
1	Full Name of the Customer	_____
2	Legal Status	<p><b>(a) Individual</b> <input type="checkbox"/></p> <p><b>(b) Other Customers</b> Corporate <input type="checkbox"/> Partnership Company <input type="checkbox"/></p> <p>Not defined above _____</p>
3	Permanent Address	_____ _____ _____
4	Business/Trading Address (If different from above)	_____ _____ _____
5	<b>In case of an "Individual Customer"</b>	<b>(2A above)</b>
	(i) Nationality	_____
	(ii) Identity No./Passport No.	_____
	(iii) Occupation or Profession	_____
	(iv) Name of Employer	_____
	(v) Location of activity	_____
	(vi) Date of Birth	_____
6	<b>In case of "Other Customers"</b>	<b>(2B above)</b>
	(i) City & Country of Incorporation Please attach Certificates as per question 11 herein	_____
	(ii) Date of Incorporation	_____
	(iii) Are any of the main Shareholders holding more than 25% in the Company	<input type="checkbox"/> YES <input type="checkbox"/> NO
	If Yes, please indicate if	Individual <input type="checkbox"/> Company <input type="checkbox"/> Other <input type="checkbox"/>

KNOW YOUR CUSTOMER (KYC) FORM

STRICTLY CONFIDENTIAL



If you have indicated "Individual" then please complete the table below and proceed to the next question, otherwise indicate herebelow the Original Beneficial Owners and answer questions (iv), (v) (vi) and (vii) and proceed to the remaining questions.

Name	ID Number/ Passport No.	Nationality	Current Resident Country	Current Business Activity	Percent age Held
1)					
2)					
3)					
4)					
5)					

(iv) Name of Stock Exchange (if Listed)

\_\_\_\_\_

(v) If the customer is a Holding company, please indicate name of any other subsidiaries/ branches/ associated companies (please supply organogram)

\_\_\_\_\_

(vi) If customer is part of a Group Company please indicate Holding Company (and please supply organogram)

\_\_\_\_\_

(vii) If customer's activities are in more than one country, please indicate names of all countries in which such activities occur and indicate volumes of Turnover per Country.

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

7 What is the principal business / activity of the Customer?

Please give details

\_\_\_\_\_

\_\_\_\_\_

8 Name of Regulator (if any)

\_\_\_\_\_

9 Please indicate name of Main Bankers and Location

Name \_\_\_\_\_ Location \_\_\_\_\_

Name \_\_\_\_\_ Location \_\_\_\_\_

Name \_\_\_\_\_ Location \_\_\_\_\_

10 **Contact Details for the Customer**

(i) Contact Person

\_\_\_\_\_

(ii) Tel

\_\_\_\_\_

Fax

\_\_\_\_\_

Mobile

\_\_\_\_\_

(iii) E-mail

\_\_\_\_\_

(iv) Website

\_\_\_\_\_

KNOW YOUR CUSTOMER (KYC) FORM

STRICTLY CONFIDENTIAL



11 Copies of Mandatory documents to be submitted by the Customer which must be certified by an authorised Certified Officer.\* Date of Certification must be within 3 months of the date of signing of this form. Copies of certified documents are not acceptable. Any documents needed to show the “Proof of Domicile” must be a Certified copy of a utility bill or tenancy agreement.

\*Note: Certification of Documents including the submission of a Proof of Domicile is only needed if the Customer is domiciled outside Cyprus.

INDIVIDUAL CUSTOMERS	OTHER CUSTOMERS	
<p><b>Individual</b></p> <p>a) Id.Card/Passport</p> <p>b) Proof of Domicile</p>	<p><b>Trust</b></p> <p>a) Trust Deed</p> <p>b) Evidence of appointment of current trustees</p> <p>c) Identity of any settlor, the trustee &amp; any principal controller who has the power to remove the trustees as well as identity of Beneficial</p>	<p><b>Companies &amp; Partnership Companys</b></p> <p>a) Company Registration Certificate</p> <p>b) Company Registration address Certificate</p> <p>c) Company Shareholder Certificate</p> <p>d) Company Directors Certificate</p> <p>e) Passport/ID copy of authorised signatory</p> <p>f) Proof of Domicile of authorised signatory</p>

12 I declare that all the answers above are true and that I have not missed, misrepresented, or omitted any important information.

I further declare that

- (a) The above mentioned Individual Customers / Other Customers do not transact any business in countries or with persons which/who are in the United States/United Nations/European Union Sanction List and in the event that they do in the future, I/we undertake to inform you immediately giving full details prior to such activity.
- (b) I/We authorise Turnkey Insurance and Reinsurance Brokers to keep all confidential and personal data and to use such only for services which they may provide to me/us and I authorise them to provide such information on a “need to know” basis to their staff for the purposes of the services which they provide to me/us as well as to any potential Insurers or Reinsurers whom they approach on my behalf.

Signature

ID Number

Date:

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Name : \_\_\_\_\_

Address : \_\_\_\_\_

Position in Company (if applicable) : \_\_\_\_\_

KNOW YOUR CUSTOMER (KYC) FORM

STRICTLY CONFIDENTIAL



**Internal Use**

Name of Employee: \_\_\_\_\_

**I regard the above KYC as a**

Normal Risk

High Risk

Low Risk

**And I recommend that this Customer**

is accepted

not accepted

referred to MOKAS

referred to CEO

For the following reasons

**Signature**

**Date:**

**Decision of CEO**

Accept the Customer

Reject the Customer

Refer to MOKAS

**Comments**

**Signature**

**Date:**

**APPENDIX 2: Internal Suspicion Report for Money Laundering and Terrorist Financing**

INFORMER'S DETAILS

Name: ..... Tel: .  
Department: ..... Fax:  
Position: .....

CLIENT'S DETAILS

Name: .....  
Address: .....  
.....  
Date of Birth: .....  
Occupation: .. .....  
Tel: .....  
Fax: .....  
Details of Employer: .....  
Passport No.: .....  
ID Card No.: .....  
Other ID Details: .....

INFORMATION/SUSPICION

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

Reason(s) for suspicion:

Informer's Signature

Date

FOR MLSCO'S USE		
Date Received:.....	Time Received:.....	.....Ref.....
Reported to MOKAS: Yes/No.....	Date Reported:.....	.....Ref.....

**APPENDIX 3: Internal Evaluation Report for Money Laundering and Terrorist Financing**

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

Informer: ..... Department:

ENQUIRIES/REFERENCES UNDERTAKEN (Brief Description) ATTACHED DOCUMENTS

MLCO's Decision

MLCO's SIGNATURE

DATE



## **APPENDIX 4: Examples of Suspicious Transactions/Activities Related to Money Laundering and Terrorist Financing**

### **A. MONEY LAUNDERING AND/OR TERRORIST FINANCING ACTIVITIES**

1. Transactions with no discernible purpose or are unnecessarily complex.
2. Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the client.
3. Large volume of transactions and/or money deposited or credited into, an account beyond the amount invoiced.
4. Settlement of the transaction by a third person which is different than the client which gave the order.
5. A client is reluctant to provide complete information when he/she establishes a business relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with Financial Organisations, names of its officers and directors, or information on its business location. The client usually provides minimum or misleading information that is difficult or expensive for the Financial Organisation to verify.
6. A client provides unusual or suspicious identification documents that cannot be readily verified.
7. A client's home/business telephone is disconnected.
8. If any person related to the client has been convicted of a criminal activity relating to money laundering or terrorist activities.