



**TDcryptottrade Services LTD**

AML & KYC Policy

Date: 16th October 2023

---

# Contents

- INTRODUCTION ..... 3
- GENERAL DEFINITIONS ..... 3
- GOVERNANCE ARRANGEMENTS ..... 6
  - 1.2 The Board of Directors, MLRO and other arrangements ..... 6
  - 1.3 Responsibilities of the Board of Directors ..... 6
  - 1.4 The Money Laundering Compliance Officer ..... 7
    - 1.4.1 Risk Based Approach ..... 9
  - 1.5.10 Client Acceptance Policy (CAP) ..... 12
  - 1.6 Client Categorization Criteria ..... 13
    - 1.6.1 Low Risk Clients ..... 13
    - 1.6.2 Medium Risk Clients ..... 13
    - 1.6.3 High Risk Clients ..... 14
    - 1.6.4 Not Acceptable Clients ..... 14
  - 1.9 Simplified Due Diligence (SDD) ..... 16
- 2 KYC DOCUMENTS REQUIREMENTS ..... 20**
  - 2.1 Time of Application of the Client Identification and Due Diligence Procedures ..... 20
  - 2.2 15 Grace Period, Failure or Refusal to Submit Information for the Verification of Clients’ Identity ..... 21
  - 2.3 Requirement to cease transactions etc ..... 21
  - 2.4 Transactions that Favour Anonymity ..... 22
  - 2.5 Physical persons accounts ..... 22
    - 2.5.1 Proof of Identity ..... 22**
    - 2.5.2 Proof of Address ..... 22**
    - 2.5.3 Natural persons residing in the Country ..... 24**
    - 2.5.4 Natural persons not residing in the Country ..... 24**
  - 2.6 Legal persons accounts ..... 24
  - 2.7 Joint Account ..... 26
  - 2.8 Trust accounts ..... 27
  - 2.9 ‘Client accounts’ in the name of a third person ..... 27
  - 2.10 Accounts of unions, societies, clubs, provident funds and charities ..... 28
  - 2.11 Accounts of unincorporated businesses, partnerships and persons with no legal substance ..... 28
  - 2.12 Investment funds, mutual funds and firms providing financial or investment services ..... 28
  - 2.13 Further Obligations for Client Identification and Due Diligence Procedures ..... 29

<b>3</b>	<b>RELIANCE ON THIRD PARTIES</b> .....	29
<b>4</b>	<b>CLIENT ACCOUNT OPENING AND MONITORING PROCEDURE</b> .....	29
<b>5</b>	<b>CLIENT ACCOUNT CLOSING AND MONITORING PROCEDURES</b> .....	30
<b>6</b>	<b>ONGOING MONITORING</b> .....	31
6.1	General .....	31
6.2	Procedures .....	31
6.3	Risk Based Approach (RBA) .....	33
6.4	Record Keeping .....	34
6.4.1	<b>General Guidelines</b> .....	34
6.4.2	<b>Records</b> .....	34
6.4.3	<b>Sanctions and penalties</b> .....	35
<b>7</b>	<b>RECOGNITION &amp; REPORTING OF SUSPICIOUS TRANSACTIONS/ ACTIVITIES TO DAML</b> .....	36
7.1	Requirements .....	36
7.2	Definition .....	36
7.3	Internal reporting .....	36
7.4	External reporting .....	36
<b>8</b>	<b>EMPLOYEES' OBLIGATIONS, EDUCATION AND TRAINING</b> .....	37
8.1	Requirements .....	37
8.2	Obligations .....	37
8.3	Training .....	38
8.4	MLRO Education and Training Program .....	38

## AML POLICIES

### Introduction

Money laundering and terrorist financing is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities including terrorist activities. This is achieved by the placement of the money launderer's cash into the financial system, by creating complex layers of financial transactions to disguise the origin of the assets and by integration of the laundered proceeds into the economy as clean money.

Money laundering is often thought of as applying to the proceeds of drugs related crime; however, terrorism and other criminal activities, including tax evasion, are equally relevant.

### General Definitions

**"Beneficial Owner"** means the natural person or natural persons, who ultimately own or control the Client and/or the natural person on whose behalf a transaction or activity is being conducted.

The Beneficial Owner shall at least include:

(a) In the case of corporate entities:

- the natural person or natural persons, who ultimately own or control a legal entity through direct or indirect ownership or control a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, a percentage of 10% plus one share to be deemed sufficient to meet this criterion; and
- the natural person or natural persons, who otherwise exercise control over the management of a legal entity.

(b) In the case of legal entities, such as foundations and legal arrangements, such as trusts, which administer and distribute funds:

- where the future beneficiaries have already been determined, the natural person(s) who is/are the beneficiary of 25%+1 of the property of a legal arrangements or entity
- where the individuals that benefit from the legal arrangement or entity have not yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates; and
- the natural person or natural persons who exercise control over 25% + 1 or more of the property of a legal arrangement or entity.

**"Business Relationship"** means a business, professional or commercial relationship which is connected with the professional activities of the Company and which was expected, at the time when the contact was established, to have an element of duration.

**"Client"** means any legal or physical person aiming to conclude a Business Relationship or conduct a single transaction with the Company. Counterparties are also treated as Clients only when the Company is executing a Client order by entering into a private Over-the-Counter deal/transaction (e.g. buying and selling) directly with the Counterparty.

**"Company"** means Future Finance Services LTD which is incorporated in the Comoros Islands with license number T2023327.

**"DAML"** means Mwali International Services Authority Department of Anti-Money Laundering for Combating Money Laundering and Terrorist Financing which is established under Part 7 of the Law.

**“European Economic Area (EEA)”** means Member State of the European Union or any other contracting state which is a party to the agreement for the European Economic Area signed in Porto on the 2nd of May 1992 and was adjusted by the Protocol signed in Brussels on the 17th of May 1993, as amended.

**“Law”** means the Anti-Money Laundering Act of 2014, as amended, of the Mwali International Services Authority of Comoros.

**“Manual”** means the Anti-Money Laundering and Combatting Financial Crime Manual (this manual).

**“Money Laundering and Terrorist Financing”** means the money laundering offences and terrorist financing offences, referred to also the following.

Every person who (a) knows or (b) at the material time ought to have known that any kind of property constitutes proceeds from the commission of a predicate offence as this is defined in Part 2 of the Law, carries out the following activities:

- Converts or transfers or removes such property, for the purpose of concealing or disguising its illicit origin or of assisting in any way any person who is involved in the commission of the predicate offence to carry out any of the above actions or acts in any other way in order to evade the legal consequences of his actions;
- Conceals or disguises the true nature, the source, location, disposition, movement of and rights in relation to, property or ownership of this property;
- Acquires, possesses or uses such property;
- Participates in, associates, co-operates, conspires to commit, or attempts to commit and aids and abets and provides counselling or advice for the commission of any of the offences referred to above;
- provides information in relation to investigations that are carried out for laundering offences for the purpose of enabling the person who acquired a benefit from the commission of a predicate offence to retain the proceeds or the control of the proceeds from the commission of the said offence; and
- commits an offence punishable by five years’ imprisonment or by a pecuniary penalty of up to €50.000 or by both of these penalties.
- Tax crimes.

**“Occasional Transaction”** means any transaction other than a transaction carried out in the course of an established Business Relationship formed by a person acting in the course of financial or other business.

**“Politically Exposed Persons (PEPs)”** means the natural persons who are or have been entrusted with prominent public functions within Country (Domestic PEPs) or outside of the Country (Foreign PEPs) and their immediate family members or persons known to be close associates of such persons.

**“Country”** means Comoros Union.

**“Regulated Market”** means a multilateral system managed or operated by a market operator and which brings together or facilitates the bringing together of multiple third-party buying or/and selling interests in financial instruments - in the system and in accordance with its non-discretionary rules - in a way that results in a contract, in respect of the financial instruments admitted to trading under its rules or/and systems, and which is authorized and functions regularly in accordance with the respective legislation.

**“Shell Bank”** means a credit institution or an institution engaged in equivalent activities incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

**“Cryptocurrency”** means a form of digital currency or virtual asset, which data are stored in digital ledger using distributed ledger technology, typically blockchain.

**“USDT”** means asset-backed cryptocurrency stablecoin issued by iFinex Inc.

**“Cryptocurrency mixer”** means a type of centralized or decentralized service, which aim is to obscure or anonymize cryptocurrency transaction - hiding the true origin of the funds.

**“Know-Your-Transaction (KYT)”** means a process that gathers information on cryptocurrency transactions and score is by risk factors

## The Money Laundering Law

The Law requires the Firm and covered institution to establish and maintain procedures to combat money laundering. This is to enable suspicions of money laundering to be recognized and reported to the authorities and for the Firm to produce its part of the audit trail to assist in official investigation.

[Future Finance Services LTD](#) (hereafter the “**Company**”) an International Brokerage and Clearing House firm established in accordance with the laws of the Comoros Union and is regulated by M.I.S.A. with Registered number T2023327, created the Manual that represents the Company’s Anti-Money Laundering and Combatting the Financing of Terrorism Manual (“**AML & CFT**”).

### 1.1.1 Purpose

The purpose of the Manual is to present the Company’s practices, measures, procedures and controls relevant to the prevention of Money Laundering and Terrorist Financing.

The Manual is developed and periodically updated by the MLCO based on the general principles set up by the Company’s Board of Directors (the “**Board**”) in relation to the prevention of Money Laundering and Terrorist Financing.

All amendments and/or changes of the Manual must always be approved by the Board.

The Manual has been prepared to comply with the all provisions of the Law.

### 1.1.2 Scope

This document complements, but does not replace:

- The Internal Procedures Manual of the Company;
- All relevant Company policies;
- Any publications referenced within the Manual.

All additional regulatory requirements that may apply in different jurisdictions should also be complied with.

### 1.1.3 Application

The Manual applies to all the services offered to the Company’s Clients as well as the relevant Company’s dealings with its Clients.

In this respect, the MLCO shall be responsible to update the Manual so as to comply with M.I.S.A.’s future requirements, as applicable, regarding the Client identification and due diligence procedures which a firm must follow.

## Governance arrangements

### 1.2 The Board of Directors, MLRO and other arrangements

#### 1.3 Responsibilities of the Board of Directors

Responsibilities of the Board in relation to the prevention of Money Laundering and Terrorist Financing include, inter alia, the following:

- To determine, record and approve the general policy principles of the Company in relation to the prevention of Money Laundering and Terrorist Financing and communicate them to the MLCO;
- To appoint a senior official that possesses the skills, knowledge and expertise relevant to financial and other activities depending on the situation, who shall act as the MLCO and where necessary, assistant MLCO's and determine their duties and responsibilities, which are recorded in this Manual;
- To approve the Manual;
- To ensure that all requirements of the Law are applied, and assure that appropriate, effective and sufficient systems and controls are introduced for achieving the abovementioned requirements;
- To ensure that the MLCO and his assistants, if any, and any other person who has been assigned with the duty of implementing procedures for the prevention of Money Laundering and Terrorist Financing (i.e. Administration/Back-Office Department personnel), have complete and timely access to all data and information concerning Clients' identities, transactions' documents (as and where applicable) and other relevant files and information maintained by the Company so as to fully facilitate in the effective execution of their duties, as included herein;
- To ensure that all employees are aware of the person who has been assigned as the MLCO, as well as his assistants (if any), to whom they report any information concerning transactions and activities for which they have knowledge or suspicion that might be related to Money Laundering and Terrorist Financing;
- To establish a clear and efficient reporting chain based on which information regarding suspicious transactions is passed without delay to the MLCO, either directly or through his assistants, if any, and notifies accordingly the MLCO for its explicit prescription in the Manual;
- To ensure that the MLCO, the assistant MLCOs, if any, and the Administration/Back-Office Department have sufficient resources, including competent staff and technological equipment, for the effective discharge of their duties.

#### **1.4 The Money Laundering Compliance Officer**

##### **(a) General Responsibilities**

The MLCO shall always be a senior official that possesses the skills, knowledge and expertise relevant to financial and other activities depending on the situation, so as to command the necessary authority. Furthermore, the MLCO shall lead the Company's Money Laundering Compliance procedures and processes.

The MLCO shall also have the resources, expertise as well as access to all relevant information necessary to perform his duties adequately and efficiently.

The level of remuneration of the MLCO shall not compromise his objectivity.

In performing his role, the MLCO shall take into account the nature, scale and complexity of the Company's business, and the nature and range of investment services and activities undertaken in the course of the business.

##### **(b) Duties of the MLCO**

During the execution of his duties and the control of the compliance of the Company with the Law, the MLCO shall obtain and utilize data, information and reports issued by international organizations.



The duties of the MLCO shall include, *inter alia*, the following:

- To design, based on the general policy principles of the Company, the internal practices, measures, procedures and controls relevant to the prevention of Money Laundering and Terrorist Financing, and describe and explicitly allocate the appropriateness and the limits of responsibility to each department that is involved in the abovementioned; It is provided that, the above includes 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 (e.g. services and transactions via the internet or the telephone) as well as measures so that the risk of money laundering and terrorist financing is appropriately considered and managed in the course of the daily activities of the Company with regard to the development of new products and possible changes in the Company's economic profile;
- To develop and establish the Client Acceptance Policy (CAP) and submit it to the Board for consideration and approval;
- To review and update the Manual as may be required from time to time, and for such updates to be communicated to the Board for their approval;
- To monitor and assess the correct and effective implementation of the policy, the practices, measures, procedures and controls and in general the implementation of the Manual. In this respect, the MLCO shall apply appropriate monitoring mechanisms (e.g. on-site visits to departments of the Company) which will provide him with 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 the MLCO identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, gives appropriate guidance for corrective measures and where deems necessary informs the Board;
- To receive information from the Company's employees which is considered to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities. The information is received in a written report form (hereinafter the "Internal Suspicion Report")
- To evaluate and examine the information received by reference to other relevant information;
- To act as a first point of contact with the DAML upon commencement of and during any investigations as a result of filing a report to the DAML;
- To ensure the preparation and maintenance of the lists of Clients categorized following a risk-based approach, which contains, among others, the names of Clients, their account number and the dates of the commencement of the Business Relationship. Moreover, the MLCO ensures the updating of the said list with all new or existing Clients, in light of any additional information obtained;
- To detect, record, and evaluate, at least on an annual basis, all risks arising from existing and new Clients, new financial instruments and services and update and amend the systems and procedures applied by the Company for the effective management of the aforesaid risks;
- To ensure that the branches and subsidiaries of the Financial Organization that operate in countries outside the Country, have taken all necessary measures for achieving full compliance with the provisions of the Law, in relation to customer identification, due diligence and record keeping procedures.
- To provide advice and guidance to the employees of the Company on subjects related to money laundering and terrorist financing;

- To acquire the required knowledge and skills for the improvement of the appropriate procedures for recognizing, preventing and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing;
- To determine the Company's departments and employees that need further training and education for the purpose of preventing money laundering and terrorist financing and organize appropriate training sessions/seminars, as well as assess the adequacy of the education and training provided;
- To prepare correctly and submit timely to the Commission the monthly prevention statement and provide the necessary explanation to the appropriate employees of the Company for its completion;
- To respond to all requests and queries from DAML, provide all requested information and fully cooperate with DAML;
- To maintain a registry which includes the abovementioned reports and relevant statistical information, the evaluation reports and all the documents that verify the accomplishment of his duties specified in the present subparagraph;
- To ensure that the branches and subsidiaries of the Company, if any, have taken all necessary measures for achieving full compliance with the provisions of the Manual, in relation to Client identification, due diligence and record keeping procedures;
- To provide advice and guidance to employees of the Company on subjects related to money laundering and terrorist financing;
- To acquire the knowledge and skills required for the improvement of the appropriate procedures for recognizing, preventing and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing;
- To determine whether the Company's departments and employees that need further training and education for the purpose of preventing Money Laundering and Terrorist Financing and organizes appropriate training sessions/seminars. In this respect, the MLCO prepares and applies an annual staff training program and assesses the adequacy of the education and training provided;
- To respond to all requests and queries from the DAML and M.I.S.A., to provide all requested information and fully cooperate with the DAML and M.I.S.A.; and
- To maintain a registry which includes relevant statistical information (e.g. the department that submitted the internal report, date of submission to the MLCO, date of assessment, date of reporting to the DAML), and all the documents that verify the accomplishment of his duties.

**The Company Policy is not to accept any cash deposits or cheque deposits and any manual deposits.**

#### **1.4.1 Risk Based Approach**

##### **(a) Approach Outline**

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

Further, the MLCO shall monitor and evaluate, on an on-going basis, the effectiveness of the measures and procedures of this Section of the Manual.

Recognizes 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 specific circumstances and characteristics;
- Helps to produce a more cost-effective system; and
- Promotes the prioritization 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 and Ancillary Services.

#### **1.4.2 Identification of Risks**

The risk-based approach adopted by the Company involves the identification, recording and evaluation of the risks that need to be managed.

The Company shall assess and evaluate the risks it faces, for the use of the Services for the purpose of Money Laundering or Terrorist Financing. The specific 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 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 DAML that the extent of measures and control procedures it applies are proportionate to the risk it faces for the use of the Services, for the purpose of Money Laundering and Terrorist Financing.

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 involve significant amounts of cash;
- Clients from high risk countries or countries known for high level of corruption or organised crime or drug trafficking; and
- Unwillingness of Client to provide information on the Beneficial Owners of a legal person.

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

- 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; and
- 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; and
- Clients introduced by a third person.

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

- Services that allow transfers to third persons/parties;
- Products or transactions which may favour anonymity

### **1.5.6 Design and Implementation of Measures and 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 CDD 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; and
- On-going monitoring of high-risk Clients' transactions and activities, as and when applicable.

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

### **1.5.7 Dynamic Risk Management**

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Clients' activities change as well as the services and financial instruments provided by the Company change. The same happens to the financial instruments and the transactions used for money laundering or terrorist financing.

In this respect, it is the duty of the MLCO 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.

### **1.5.8 Relevant International Organizations**

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 MLCO and the Administration/Back-Office Department shall consult data, information and reports

[e.g. Clients from countries which inadequately apply FATF, country assessment reports] that are published in the following relevant international organizations:

- FATF - [www.fatf-gafi.org](http://www.fatf-gafi.org);
- The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (hereinafter “MONEYVAL”) - [www.coe.int/moneyval](http://www.coe.int/moneyval);
- The EU Common Foreign & Security Policy (CFSP) - [eeas.europa.eu/cfsp/](http://eeas.europa.eu/cfsp/);
- The UN Security Council Sanctions Committees- [www.un.org/sc/committees](http://www.un.org/sc/committees);
- The International Money Laundering Information Network (IMOLIN) - [www.imolin.org](http://www.imolin.org); and
- The International Monetary Fund (IMF) – [www.imf.org](http://www.imf.org).
- Office of Foreign Assets Control - [www.treasury.gov](http://www.treasury.gov)
- Transparency International Corruption Perceptions Index - [www.transparency.org/](http://www.transparency.org/)
- World Bank Group - [www.worldbank.org/](http://www.worldbank.org/)

### **1.5.9 Country Risk Methodology**

Regarding client risk classification, the company implement the calculation methodology of Country risk. As per this approach, all countries are risk assessed based on a number of internationally recognised sources. Country risk is calculated based on the risk score provided by each of the below sources plus inheritance risk:

- Basel AML Index
- Corruption Perceptions Index – Transparency International
- Countries subject to a FAFT call for action
- FATF monitored jurisdictions with strategic deficiencies
- Not EU or equivalent jurisdiction countries as per Commission Implementing Decision (EU) 2016/230 of 17 February 2016

If there are no data available from the sources referred above, the 90% of the worst rating is applied. The overall score counts towards the assignment of the specific client AML score and the client Risk Categorization (High, Medium, Low)

Furthermore, the Company proceeded with the categorization of clients residing in a Jurisdiction subject to a FATF call as “High-High”.

### **1.5.10 Client Acceptance Policy (CAP)**

#### **(a) General Principles of the CAP**

The Company’s Client Acceptance Policy (hereinafter the “CAP”), in accordance with the principles and guidelines described in AML Manual, defines the criteria for accepting new Clients and stipulates the

Client categorization criteria which shall be adhered to by the Company and especially by the employees and third parties who are involved in the Client Account Opening process. The said policy should be revised on an annual basis.

The General Principles of the CAP are the following:

- 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;
- Where the Client is a prospective Client, an account can be activated only after the relevant due diligence and identification measures and procedures have been conducted;
- All documents and data must be collected before accepting a new Client;
- No account shall be opened in anonymous or fictitious names(s); and
- No PEP account shall be opened unless the prospective Client is approved by a member of the Board.

### **1.6 Client Categorization Criteria**

The Company shall conduct a Business Wide Risk Assessment (“BWRA”) by taking into consideration its client’s risk (economic profile, customer risk, product or service risk and geographical risk), complexity and structure of the business, products and services offered by the Company and the payment methods accepted by the Company, to identify, assess and understand all the ML/FT risks the Company is exposed to and proceed with the implementation of the Risk Based Approach that shall be followed by the Company for the risk categorization of the clients.

The aim of the BWRA is ultimately to enhance the efficiency of the allocation of resources across the anti-money laundering and combating the financing of terrorism regime and ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the risks identified.

This methodology shall provide quantitative results to assist in the decision-making process towards the level of risk or threat that the clients’ business relationship entails. Based on that methodology, the MLRO shall introduce a risk mitigation plan and implemented controls based on the different risk-levels for the on-going due diligence on customers.

Due to the non-face-to-face nature of the business, the Company’s customers shall automatically be categorised as high-risk, except for cases where face-to-face meetings may take place; however, such customers may still be categorised as high risk due to other criteria. Furthermore, the Company shall proceed in sub-categorising the high-risk clients in high, normal and low risk.

Following the categorization of the clients the Company should proceed in performing the relevant Due Diligence.

#### **1.6.1 Low Risk Clients**

The Company has to gather sufficient information to establish if the Client qualifies as a low-risk Client. In this respect, the MLCO shall be responsible to gather the said information. The said information shall be duly documented and filed, as applicable, according to the recording keeping procedures of the Company.

The Company shall follow the *Simplified Client Identification and Due Diligence Procedures* for low risk Clients.

#### **1.6.2 Medium Risk Clients**

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

TDcryptotrade Services LTD is regulated as International Brokerage and Clearing House by M.I.S.A. under license number T2023327 Registered Address: Bonovo Road, Fomboni, Island of Moheli, Comoros Union

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

### 1.6.3 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 and/or European Commission;
- 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; and
- Any other Client determined by the Company itself to be classified as such

The Company shall apply the *Enhanced Client Identification and Due Diligence* measures for high risk Clients and the due diligence and identification procedures for the specific types of high-risk Clients as explained below.

### 1.6.4 Not Acceptable Clients

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 their identity and the creation of their economic profile, without adequate justification;
- Shell Banks;
- Customers residing in restricted jurisdictions including Japan, Canada and USA;
- Customers subject to prohibitions imposed by decisions of the European Union, the national authorities of the countries where Group Companies are established or other international organizations;
- Customers for whom reports of unusual or suspicious transactions are repeatedly submitted to the DAML;
- Customers whose activities or transactions are not consistent with the information available on them, their professional activity, their risk profiles and the origin of the funds;
- Gambling and betting companies (including companies with similar activities offered through the Internet) operating without authorization or supervision;
- Customers providing financial or insurance services without authorization or control by a supervisory authority.
- Clients which would be classified PEP.

## 1.7 Customer Due Diligence (CDD) requirements

The Firm must apply CDD measures to a customer when it:

- When establishing a Business Relationship;

- When carrying out Occasional Transactions amounting to 10,000 USDT or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- When there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction;
- When there are doubts about the veracity or adequacy of previously Client identification data.

In general, the ‘customer’ for this purpose will be the party, or parties, with whom the business relationship is established, or for whom the transaction is carried out.

If in doubt as to which information must be obtained to verify a new client’s identity, the employee must consult the MLRO for guidance without delay and prior to commencing any dealings.

### **1.8 Construction of Economic Profile, Client Identification & Due Diligence Principles**

Construction of the Client’s economic profile needs to include/follow the principles below:

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 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;
- A person’s residential and business address will be an essential part of his identity;
- The Company will never use the same verification data or information for verifying the Client’s identity and verifying his/her home address.

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; and
- 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-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; and
  - 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);
- 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; and
  - 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. Transactions that 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 MLRO and then by the latter to the DAML.

The Company shall apply each of the CDD measures and identification procedures set out above but may determine the extent of such measures on a risk-sensitive basis depending on the type of Client, Business Relationship, product or transaction.

For the purposes of the provisions relating to identification procedures and CDD 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.

The construction of the Client's economic profile according to the provisions above shall be undertaken by the MLRO.

In this respect, the data and information collected for the construction of the economic profile shall be fully documented and filed, as applicable, by the Administration/Back-Office Department.

## **1.9 Simplified Due Diligence (SDD)**

The following shall apply:

- Identify the customer and verify the customer's identity on the basis of documents, data or information obtained from a reliable and independent source
- The Company may not apply the enhance due diligence measures for a Client who may be categorised as a low risk Client.
- Furthermore, where the Client is categorised as a low risk Client, the verification of the identity of the Client and the Beneficial Owner may be completed during the establishment of a Business Relationship if this is necessary not to interrupt the normal conduct of business and where the risk of money laundering or terrorist financing occurring is low. In such situations these procedures shall be completed as soon as possible after the initial contact and before any transactions are conducted;

- When assessing the abovementioned information, the Company shall pay special attention to any activity of those Clients or to any type of transactions which may be regarded as particularly likely, by its nature, to be used or abused for money laundering or terrorist financing purposes.
- The Company shall not consider that Clients or transactions described in the first point above, represent a low risk of money laundering or terrorist financing if there is information available to suggest that the risk of money laundering or terrorist financing may not be low;
- Where there is a 'beneficial owner' who is not the customer, identify the beneficial owner and take adequate measures, on a risk-sensitive basis, to verify his identity so as to be satisfied that it knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement;
- Obtain information on the nature and intended purpose of the business relationship

SDD does not exempt the Firm from the obligation to verify identity where it knows or suspects that a proposed relationship or occasional transaction involves money laundering or terrorist financing, or where there are doubts about the veracity or accuracy of documents, data or information previously obtained for the purposes of customer verification.

Once SDD has been applied to a customer, it will be necessary for the Firm to conduct certain ongoing monitoring of the relationship with a view to checking that the basis for applying SDD remains appropriate.

If there is any doubt as to whether it is appropriate to proceed on the basis of having performed SDD, then the MLRO should be consulted.

Where SDD is applicable, the customer must be identified, their identity should be recorded, and evidence should be kept as to why it has been determined that the customer falls into one of the relevant categories which justify SDD.

### **1.11 Enhanced Client Identification and Due Diligence (High Risk Clients)**

The Firm must apply 'enhanced' due diligence measures and ongoing monitoring, on a risk-sensitive basis, in specified circumstances, including

- (a) Where the Client has not been physically present for identification purposes, the Company shall apply one or more of the following measures:
  - Take supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution; and
  - Telephone contact with the customer at his home or office, on a telephone number which has been verified from independent and reliable sources;
  - Communication via video call with the customer, provided the video recording and screen shot safeguards apply to the communication. It is provided that a customer, whose identity was verified hereunder cannot deposit an amount over 5,000 USDT per annum;
  - Communication with the customer through an address that the Company has previously verified from independent and reliable sources, in the form of a registered letter.

Please note that the Company will use two sources of electronic verification which their electronic data bases include a wide range of sources with information from different time periods with real-time update and trigger alerts when important data alter.

- (b) With respect to transactions or Business Relationships with PEPs

A PEP is defined as 'an individual' means the natural persons who are or have been entrusted with prominent public functions within Country (Domestic PEPs) or outside of the Country (Foreign PEPs) and their immediate family members or persons known to be close associates of such persons.

The company will not accept any client classified as PEP. In case client will become PEP during his business relationship with the company, company will close his account.

The Company shall also be 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;

Below are described due diligence and identification procedures with respect to high risk Clients.

### **1.12 Trusts**

Identity: The Firm should obtain the following information:

- (i) full name of the trust,
- (ii) nature and purpose of the trust (e.g. discretionary, testamentary, bare),
- (iii) country of establishment,
- (iv) names of all trustees,
- (v) names of any beneficial owners and
- (vi) name and address of any protector or controller.

Verification: The identity of the trust must be verified using reliable and independent documents, data or information. This may require sight of relevant extracts from the trust deed, or reference to an appropriate register in the country of establishment. The Firm must take measures to understand the ownership and control structure of the customer.

The Firm should take appropriate steps to be reasonably satisfied that the person the Firm is dealing with is properly authorized by the customer. Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

### **1.13 Non face-to-face Clients**

Due to the non-face-to-face nature of business, the Company's customers are automatically categorised as high-risk, except for cases where face-to-face meetings may take place, however such customers may still be categorised as high risk due to other criteria. Furthermore, the Company proceeds in sub-categorising the high-risk clients in high, medium and low risk based on other factors.

The MLRO shall apply the following with respect to non-face-to-face Clients:

- When a Client, requests the establishment of a Business Relationship or an Occasional Transaction through mail, telephone, or the internet without presenting himself for a personal interview, the Company must follow the established Client identification and due diligence procedures, as applied for Clients with whom it comes in direct and personal contact and obtain exactly the same identification information and documents;

- However, due to the difficulty in matching the Client with the collected identification data, the Company shall apply enhanced Client identification and due diligence measures, so as to effectively mitigate the risks associated with such Business Relationship or Occasional Transaction.

The MLRO shall apply enhanced due diligence measures with respect to the Clients categorized as high-risk Clients according to the criteria set above.

#### **1.14 “Politically Exposed Persons” (PEP) accounts**

The establishment of a Business Relationship or the execution of an Occasional Transaction with persons holding important public positions and with natural persons closely related to them, may expose the Company to enhanced risks, especially if the potential Client seeking to establish a Business Relationship.

The meaning ‘**Politically Exposed Persons**’ includes the following natural persons who are or have been entrusted with prominent public functions’ in Country or outside of Country:

- Heads of State, heads of government, ministers and deputy or assistant ministers;
- Members of parliaments;
- Members of the governing bodies of political parties;
- Members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- Members of courts of auditors or of the boards of central banks;
- Ambassadors, charges des affaires and high-ranking officers in the armed forces;
- Members of the administrative, management or supervisory bodies of State-owned enterprises;
- Directors, deputy directors and members of the board or equivalent function of an international organization;
- Central Financial Institutions: Examples here would be the Court of Auditors and members on the boards of central banks;
- Armed Forces: In this situation a PEP rating would typically only apply to a high-ranking officer;
- International Sports Committees: Members of these committees may be influenced to vote on the location of major sporting events/contracts for building venues, etc., so have recently been included by FATF under their definition of a PEP;
- Mayors
- Anyone who has a close business relationship or joint beneficial ownership of legal entities or legal arrangements with a PEP;
- Anyone who has the sole beneficial ownership of a legal entity which is known to have been set up for the benefit de facto of the PEP;
- Parents and children of PEPs, Spouse or partner, Siblings, Uncles and aunts, even slightly indirect family members (such as in-laws) will be considered as a politically exposed person.

‘**Immediate family members**’ includes the following:

- The spouse or the person with which cohabit for at least one year;
- The children and their spouses or the persons with which cohabit for at least one year; and
- The parents.

‘**Persons known to be close associates**’ includes the following:

- Any natural person who is known to have joint Beneficial Ownership of legal entities or legal arrangements, or any other close business relations, with a person described above;
- Any natural person who has sole Beneficial Ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person described above.

**The company will not accept any client classified as PEP. In case client will become PEP during his business relationship with the company, company will close his account.**

### **1.15 Clients from countries which inadequately apply FATF's recommendations**

- The FATF 40+9 Recommendations constitute the primary internationally recognized standards for the prevention and detection of Money Laundering and Terrorist Financing.
- The Company shall apply the following with respect to Clients from countries which inadequately apply FATF's recommendations:
  - Exercise additional monitoring procedures and pay special attention to Business Relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or apply inadequately the aforesaid 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 the DAML ; and
  - With the aim of implementing the above, the Head of the Administration/Back-Office Department and the MLRO shall consult the country assessment reports prepared by the FATF (<http://www.fatf-gafi.org>), the other regional bodies that have been established and work on the principles of FATF [e.g. Moneyval Committee of the Council of Europe ([www.coe.int/moneyval](http://www.coe.int/moneyval))] and the International Monetary Fund ([www.imf.org](http://www.imf.org)). Based on the said reports, the MLRO assesses the risk from transactions and Business Relationships with persons from various countries and decides on the countries that inadequately apply the FATF's recommendations. According to the aforesaid decision of the MLRO, the Company applies, when deemed necessary, enhanced due diligence measures for identifying and monitoring transactions of persons originating from countries with significant shortcomings and strategic deficiencies in their legal and administrative systems for the prevention of Money Laundering and Terrorist Financing.

## **2 KYC Documents Requirements**

### **2.1 Time of Application of the Client Identification and Due Diligence Procedures**

With respect to the timing of the application of the Client Identification and Due Diligence Procedures, the MLRO shall be responsible for the application of the following provisions:

- (a) The verification of the identity of the Client and the Beneficial Owner shall be performed **before the establishment** of a Business Relationship or the carrying out of a transaction; it is noted that the identification procedure includes the following (where appropriate):
  - creation of an economic profile for the client/beneficial owner and/or,
- (b) By way of derogation from point (a) above, the verification of the identity of the Client and the Beneficial Owner may be completed during the establishment of a Business Relationship if this is necessary not to interrupt the normal conduct of business, where the risk of money laundering or terrorist financing occurring is low and where the process of verifying the procedure is completed as soon as practicable after the initial contact. The obligation of not trading will be excluded only

in the cases where the above conditions apply. The Policy of the Company is to proceed with full verification of the identity of the Client before the establishment of a Business Relationship with the client;

- (c) In cases where the Company is unable to comply with the abovementioned requirements, the Company shall not carry out any transaction through a bank account, establish a Business Relationship or carry out an Occasional Transaction and consider making a report to the DAML ; and
- (d) Identification procedures and CDD requirements shall be applied not only to all new Clients but also to existing Clients at appropriate times, depending on the level of risk of being involved in money laundering or terrorist financing.

## **2.2 15 Grace Period, Failure or Refusal to Submit Information for the Verification of Clients' Identity**

- **15 Grace Period**

The company has a full understanding of Circular C143 and C157 issued in 2016, with respect to the timing of the application of the Client Identification and Due Diligence Procedures and in respect to that the company, has established the 15 Days Grace period procedure which allows clients to submit all necessary document within 15 days after their first deposit up to 5,000 USDT.

On the 16<sup>th</sup> day if a client failed or refuse to submit the necessary documents, in case of open positions will be requested to be closed, amount deposited will be refunded and the account will be terminated. In case where a client deposit more than 5,000 USDT, he/she cannot proceed with any trade unless the company and the verification team will fully proceed to the client's verification.

The company implements, where appropriate, in view of the client's verification procedure undertaken in the course of the business relationship, adequate automated electronic management information system which is supplying all necessary departments on a timely basis, all valid and necessary information for each department, to follow the procedure.

- **Failure or Refusal to Submit Information**

Failure or refusal by a Client to submit, within the 15 grace period or 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 while at the same time the MLRO considers whether it is justified under the circumstances to submit a report to the DAML .

If, during the Business Relationship, a Client fails or refuses to submit, within a reasonable timeframe, the required verification data and information, the Company and the MLRO shall consider terminating the Business Relationship and close all the accounts of the Client, taking also into account the specific circumstances of the Client in question and the risks faced by the Company on possible money laundering and/or terrorist financing, while at the same time examine whether it is justified under the circumstances to submit a report to DAML .

## **2.3 Requirement to cease transactions etc**

Where it is not possible to apply the CDD measures, the Firm must not carry out a transaction with or for the customer through a bank account; must not establish a business relationship or carry out an

occasional transaction; must terminate any existing business relationship; and must consider whether to make a disclosure to the DAML

The Firm is prohibited from setting up anonymous accounts for any new or existing customer. If the Firm concludes that the circumstances do give reasonable grounds for knowledge or suspicion of money laundering or terrorist financing, a report must be made to the DAML.

## **2.4 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 authorized 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 authorized signatory of the account.

## **2.5 Physical persons accounts**

### **Client identification process performed prior to opening new accounts:**

Prior to accepting new clients and allowing them to trade with the Company, the following documents shall be obtained:

#### **2.5.1 Proof of Identity**

A government-issued document which incorporates: the customer's full name and photograph and either his residential address or his date of birth.

POI needs to be a clear copy of one of the following governments issued Identification document:

- a) Passport
- b) National Identification Number
- c) Driver's license

POI must clearly show the following details:

- a) Photo
- b) Full name
- c) Date of birth (DoB)
- d) Expiration date
- e) Document number
- f) Full security strip (if applicable)

The Compliance Call is an extra measure of verification and is executed on a daily basis and for all languages for the Clients who make a deposit. In the compliance call we verify the identity of the client; hence we check whether his personal details are correct or not, and we also inform him about our main policies and about our Terms & Conditions.

#### **2.5.2 Proof of Address**

A utility bill, house deed, or bank statement not older than three (3) months, stating the client's name and residential address. In cases where the clients are operating within countries where the addresses are identified only by reference to a P.O. Box, a declaration letter signed by an independent government representative or professional officer (such as post office, lawyer, accountants and notary public) confirming the client's address is accepted. Moreover, in cases where the clients are living with a family member and the only proof of address they can produce is in the name of the relative, a declaration confirming the family relationship is accepted to verify the validity of the proof of address provided.

In addition, personal details of the client are verified through information provided by the payment service provider (e.g. bank, credit card company) to ensure that they are identical to the information provided by the client during the application process.

The following documents shall be considered acceptable:

- Recent Utility Bill (i.e. electric, water, telephone, gas) - The bill must be less than three (3) months old. Please note that a mobile phone will be accepted as a valid Proof of Residence only if the name on the bill matches the name of the registration and same for the telephone number.
- Recent Mortgage Statement
- Signed Lease Agreement still within term
- Bank, Investment Letter
- Deed or Other Evidence of Property
- Bill for Homeowner's or Renter's Insurance Policy (less than three (3) months old)
- Security System Bill/Statement (less than three (3) months old)
- Government-Issued Letters or Statements Establishing Current Address (less than twelve (12) months old)
- Domestic Passport for Russians and Ukrainians (make sure that the address is matching the one mentioned in the registration)

**(NOTE** that any document that has been used for proof of identity cannot also be used as proof of address - excepting the Domestic Passport mentioned above. Furthermore, all documents provided in any other language excepting English should be translated. Translation Form should be provided for each non-English document.)

- Recent Bank Statement - Must be less than three (3) months old

**(Important:** Screen shots of bank statements are only acceptable in cases where the bank account being used for proof of address is the same as the one used to fund the account.)

For example:

- Tax Letters and notices
- Letters or notices from government housing authorities
- Jury duty notices
- Voter registration notices
- Other official government letters or notices showing customer name and address being verified

**The proof of residence must:**

- Show current address
- Show name as indicated on the account application
- Be from a credible source (with a visible logo)
  
- Be dated within the last three (3) months

**NOTE:** P.O. Box as Proof of Residence is not acceptable.

The Following are acceptable as other forms of Proof of Residence for the locals:

- Proof of residence from Land registry given that proof of previous address is also provided.

The Following are acceptable as other forms of Proof of Residence for non-locals:

- Valid Lease Agreement (valid for the current year) between the client and the land lord or between the company which employ our client and the land lord associated with the contract of employment or a letter from the company declaring our client employment duly signed by the company.



### **2.5.3 Natural persons residing in the Country**

The Company shall obtain the following information to ascertain the true identity of the natural persons residing in the Country:

- True name and/or names used as these are stated on the official identity card or passport;
- Full permanent address in the Country, including postal code;
- Telephone (home and mobile) and fax numbers;
- Email address, if any;
- Date and place of birth;
- Nationality; and
- Details of the profession and other occupations of the Client including the name of employer/business organisation.

In order to verify the Client's identity/name, the Company shall request the Client to present a copy of the original document which is issued by an independent and reliable source that carries the Client's photo (e.g. Passport, National Identity cards, Driving License etc).

The Client's permanent address shall be verified using one of the following ways:

- The production of a recent (up to 3 months) utility bill, local authority tax bill or a bank statement or any other document same with the aforesaid.

### **2.5.4 Natural persons not residing in the Country**

The Company shall obtain the information described above to ascertain the true identity of the natural persons not residing in the Country.

In addition, and without prejudice to the application on a risk-sensitive basis, the Company shall require and receive information on public positions which the prospective Client holds or held in the last twelve (12) months as well as whether he is a close relative or associate of such individual, in order to verify if the Client is a PEP.

Furthermore, passports shall always be requested from the Clients not residing in the Country and, if available, official national identity cards issued by the competent authorities of their country of origin shall be obtained. Certified true copies of the pages containing the relevant information from the said documents shall also be obtained and kept in the Client's files.

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

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 respect, passport's number, issuing date and country as well as the Client's date of birth always appear on the documents obtained, so that the Company would be in the position to verify precisely whether a Client 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

## **2.6 Legal persons accounts**

A different identification procedure is followed for legal persons interested in opening an account with the Company. The documentation that needs to be obtained by the corporate client is presented below:

TDcryptotrade Services LTD is regulated as International Brokerage and Clearing House by M.I.S.A. under license number T2023327 Registered Address: Bonovo Road, Fomboni, Island of Moheli, Comoros Union

For Clients that are legal persons, the Company shall establish that the natural person appearing to act on their behalf, is appropriately authorised to do so and his identity is established and verified according to the procedures outlined above.

The Company shall take 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 according to the procedures outlined above. 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 authorised 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 an EEA country or a third country with equivalent disclosure and transparency requirements;
- The registered shareholders that act as nominees of the Beneficial Owners; and
- The economic profile of the legal person.

**(a) Verification of the natural person which is acting on behalf of the legal entity:**

- Board resolution authorizing the person to act on behalf of the company;
- Copy of the passport and utility bill of that person;

**(b) Full ascertainment of the legal entity's control and ownership structure and verification of the identity of the beneficial owners and those who exercise control over the legal entity:**

- If a regulated entity, copy of the license and copy of directors' certificate;
- If not regulated entity, legal structure (if part of a group of companies) and KYC documents for all beneficial owners holding more than 25% of the share capital (25% plus 1);

**(c) Verification of the identity of the legal entity:**

- Certificate of incorporation and certificate of good standing;
- Certificate of registered office;
- Certificate of directors and secretary;
- Certificate of shareholders;
- Certificate of Incumbency, if applicable (shall replace certificates of incorporation, registered office, directors and secretary and shareholders);
- Memorandum and articles of association (if not EU regulated or regulated in a country with equivalent disclosure and transparency requirements);
- In case that registered shareholders act as nominees of the beneficial owners, a copy of the trust agreement concluded between the nominee shareholder and the beneficial owners;
- Documents for the verification of the identity of the registered shareholders and the beneficial owners (passport and utility bill).

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

As an additional due diligence measure, on a risk-sensitive basis, the Company shall carry out (when deemed necessary) a search and obtain information from the records of the Companies House (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 Companies House of the Country or by an appropriate authority outside the Country

It is pointed out that, if at any later stage any changes occur in the structure or the ownership status or to any details of the legal 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.

In the case of a Client-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 Country or abroad, the Company, before establishing a Business Relationship or executing an Occasional Transaction, shall verify the ownership structure and the identity of the natural persons who are the Beneficial Owners and/or control the other legal person.

Apart from verifying the identity of the Beneficial Owners, the Company shall identify the persons who have the ultimate control over the legal person's business and assets.

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 authorisation and who would be in a position to override the internal procedures of the legal person, the Company, shall verify 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 more than 25% in the legal person's ordinary share capital or voting rights.

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 Country or abroad, the Company shall implement the following procedure:

- The Company shall 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;
- Furthermore, the Company shall 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.

## **2.7 Joint Account**

A joint account is made between 2 clients. Both clients should be fully verified in order to proceed with the approval.

Once we receive the internal Joint Account Application Form, we check if it is filled and signed by both clients.

- Married Couples – Proof of marriage is required;
- 1st Degree Family Related – Proof such as birth certificate is required;

- Non-related but having a joint bank account – Joint bank account statement is required and proof of relationship.

In most cases, both account holders will submit the documents mentioned above for individuals. If additional documents are required, client will be contacted via email.

## **2.8 Trust accounts**

The MLRO shall apply the following with respect to trust accounts:

- When the Company establishes a Business Relationship or carries out an Occasional Transaction with trusts, it shall 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 prescribed in throughout this policy;
- Furthermore, the Company shall 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 shall be recorded and kept in the Client's file.

## **2.9 'Client accounts' in the name of a third person**

The MLRO shall apply the following with respect to "Client accounts" in the name of a third person:

- The Company may open "client accounts" (e.g. omnibus accounts) in the name of financial institutions from EEA countries.

In case the Company receives a request to open "client accounts" (e.g. omnibus accounts) in the name of financial institutions originating from countries other than the EEA, then the Company shall examine such requests on a case by case basis and shall undertake additional due diligence measures on such financial institutions. Such additional measures shall include a country-profile assessment in terms of AML reputation and legislation, analysis of the AML measures applied by such financial institutions, whether the financial institution is supervised in terms of AML, analysis of the line of business and clientele type of the financial institution and any additional measures deemed necessary during the assessment. It is stressed that the Company shall be extra vigilant on such cases.

- In the case that the opening of a "client account" is requested by a third person acting as an auditor/accountant or an independent legal professional or a trust and company service provider situated in a country of the Company shall proceed with the opening of the account provided that
- the following conditions are met:
  - The third person is subject to mandatory professional registration in accordance with the relevant laws of the country of operation;
  - The third person is subject to regulation and supervision by an appropriate competent authority in the country of operation for Anti-Money Laundering and Terrorist Financing purposes;
  - The MLRO has assessed the Client identification and due diligence procedures implemented by the third person and has found them to be in line with the Law. A record of the assessment should be prepared and kept in a separate file maintained for each third person; and
  - The third person makes available to the Company all the data and documents described in this Policy/Manual.

## **2.10 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 shall obtain a list of the members of board of directors'/management committee of the abovementioned organisations and verifies the identity of all individuals that have been authorised to manage the account.

## **2.11 Accounts of unincorporated businesses, partnerships and persons with no legal substance**

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 shall be verified according to the procedures outlined above.

In addition, in the case of partnerships, the original or a certified true copy of the partnership's registration certificate shall be obtained.

The Company shall obtain documentary evidence of the head office address of the business, ascertains the nature and size of its activities and receives all the information required for the creation of the economic profile of the business.

The Company shall request, in cases where it exists, the formal partnership agreement and shall also obtain mandate from the partnership authorising the opening of the account and confirming authority to a specific person who will be responsible for its operation.

## **2.12 Investment funds, mutual funds and firms providing financial or investment services**

The Company shall establish and maintain Business Relationships or execute Occasional Transactions with persons who carry out such services and activities. Such persons must:

- (a) Possess the necessary license or authorisation from a competent supervisory/regulatory authority of the country of their incorporation and operation to provide the said services; and
- (b) Be subject to supervision for the prevention of Money Laundering and Terrorist Financing purposes.

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 Company shall request and obtain, in addition to the abovementioned, in previous points, documentation and the information required by the Manual for the identification and verification of persons, including the Beneficial Owners, the following:

- A copy of the license or authorisation 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 in order to fully understand the control structure and management of the business activities as well as the nature of the services and activities provided by the Client.

In the case of investment funds and mutual funds the Company, apart from identifying Beneficial Owners,

shall obtain 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.

## **2.13 Further Obligations for Client Identification and Due Diligence Procedures**

In addition to the principles described above, the Company, and specifically the MLRO shall:

- Ensure that the Client identification records remain completely updated with all relevant identification data and information throughout the Business Relationship;
- 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.

Despite the aforementioned obligations and while taking into consideration the level of risk, if at any time during the Business Relationship, the Company becomes aware that reliable or adequate data and information are missing from the identity and the economic profile of the Client, then the Company takes all necessary action, by applying the Client identification and due diligence procedures according to the Manual, 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.

In addition to the above obligations, the Company shall check 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 and/or significant 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; and
  - change of the principal trading partners and/or undertaking of major new business activities;
  - a material change in the way and the rules the Client's account operates, such as:
    - ✓ change in the persons that are authorised to operate the account; and
    - ✓ application for the opening of a new account for the provision of new investment services and/or financial instruments.

## **3 Reliance on third parties**

The Firm may rely on specified types of person to apply the CDD measures, provided that the third-party consents to being relied on. However, the Firm, not the third party, remains liable for any failure to apply the due diligence measures.

## **4 Client account Opening and Monitoring Procedure**

The Client Account Opening and Monitoring Procedures shall be undertaken by the MLRO. In general terms, responsible for the following:

- (a) Assisting with the maintenance and updating of the Client account opening procedures;
- (b) Monitoring the maintenance and update of the Client account opening procedures by the Customer Support Department, as applicable;

- (c) Providing Company information to the Clients (terms of business of the Company), including the Company's order execution policy and policy to act in the best interest of Clients;
- (d) Assisting with the conduct of the due diligence procedures during the account opening stage ("Know-Your-Client" – KYC - procedures);
- (e) Monitoring the performance at the account opening stage ("Know your Client" procedures) by the Customer Support Department, as applicable;
- (f) Implementing the Client categorisation procedure;
- (g) Implementing the Appropriateness and Economic Profile Questionnaire and determining the assessment of the expertise, experience and knowledge of the Client;
- (h) Following the approval of a Client account and for the duration of the account operation, monitoring Clients regarding suspicious transactions, whereas these do not match with their investment profile and notify the MLRO;
- (i) Checking Client relationship *inter se*, if any
- (j) Ensure that Clients are informed in writing that their personal details shall not be used for any other purposes other than the provision of the services specified in the Client Agreement;
- (k) Ensure that Client Agreements were delivered to Clients;
- (l) Record keeping and documentation filing of Client Agreements and all the relevant documentation ("Know-Your-Client" – KYC - procedure documents).

## 5 Client Account Closing and Monitoring Procedures

The User's account maybe Suspended or terminated by either party upon giving the other party written notice of Suspension or termination, which will take effect immediately, unless otherwise specified in the notice.

In the event of client's account termination, any Open Positions should be closed by the client as soon as reasonably practicable and in any event no longer than 7 (seven) calendar days after the client's written notice.

Upon the termination of an account, all outstanding monies by the Client to the Company will become immediately due and payable including but not limited to:

- (a) Fees and charges;
- (b) Administrative expenses incurred for terminating the account;
- (c) Any losses and/or expenses realised in closing out open transactions or settling or concluding outstanding obligations incurred by the Company.

All outstanding funds by the Client to the Company, shall be deducted from the Client's Account before transferring any credit balances to Client. Transferring of monies to the Client shall be postponed until all outstanding obligations have been settled. Furthermore, the Company shall be entitled to require from the Client to pay any charges and/or fees incurred in transferring investments.

In the event that the client withdraws all funds from the client's Trading Account and cease trading activity without closing the Trading Account, then the account will be designated as "Inactive Account" as described in detail in Inactive and Dormant Account Policy.

Furthermore, according to the Inactive and dormant Account policy, when a client withdraws funds or the total equity is 0 and there are no "activities", as is described in detail in the Inactive and Dormant Account Policy, the account will be terminated.

A Client's Account might be closed due to the following reasons:

- (a) Client's request;
- (b) Suspicion of Fraud or abusive behaviour;
- (c) Failure to provide documents required by the AML Compliance Department within a reasonable timeframe;
- (d) Failure to provide updated documents requested by the AML Compliance Department within a reasonable timeframe;
- (e) Breach of the Company's Terms and Conditions;
- (f) Regulatory Reasons;
- (g) Dormant Account

## **6 Ongoing Monitoring**

### **6.1 General**

The Firm must monitor its business relationships on an ongoing basis, which means scrutinising transactions including, where necessary, the source of the funds, and keeping the documents, data or other information obtained for applying due diligence measures up to date.

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 to the DAML.

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.

In this respect, the MLRO shall be responsible for maintaining as well as developing the on-going monitoring process of the Company.

### **6.2 Procedures**

The procedures and intensity of monitoring Clients' accounts and examining transactions on the Client's level of risk shall include the following 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 (e.g. the Head of the Brokerage Department) shall be responsible to communicate with the MLRO;
- Suspicious transactions and screening of all Clients ware for passport verification, PEP Research, sanctions lists, profile checking and risk assessment;
- Furthermore, the investigation of unusual or suspicious transactions by the MLRO.;
- The ascertainment of the source and origin of the funds credited to accounts;
- The use of appropriate and proportionate IT systems, including:



- Adequate automated electronic management information systems which will be capable of supplying the Board of Directors and the MLRO, 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; 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;
- 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;
- 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;
- The monitoring also covers clients who do not have a contact with the Company, as well as dormant accounts exhibiting unexpected movements;
- Notify customers, through their last known address, that their account has been left dormant for some period, with no financial activity or full and proper data update

and that their data must be updated, and transactions must be undertaken within the specified period, provided that the notice includes a description of the consequences of noncompliance with the specified time period.

- If the time period expired with no financial activity or data update, the company shall take these actions (within two working days):
  - Classify the account as dormant and prohibit transactions;
  - Maintain balances and make them available and not act upon them without instructions from the customer, or the relevant authorities;
  - Supply customers, through their last known address, with a final account statement and clarify that no further account statements shall be sent until they contact the company for account activation;
  - If the account is classified as dormant, customers can contact the Company to activate the account and make the necessary updates;
  - Clients who do not wish to have the account activated, must contact the Company in order to close the account and have their available balance returned to the source and/or contact the relevant market concerning their securities dues, without violating the Company's right to close the account, taking into consideration the account opening agreement;
  - Duplicate accounts may be accepted only for the following legitimate reasons:
    - Different base cryptocurrency
    - Different leverage

- Different trading strategy / trading different products
- Requires clean history on account
- Wants to carry out back testing on old account and trade on new one.

Clients should be restricted to 3 accounts up to a maximum of 5 for exceptions. Dealing should authorize any additional account only after checking trading on existing account. All accounts MUST be under the same email account and where possible client should close previous accounts not being used.

Clients are automatically turned in Dormant Account (when criteria are met) and Customer Support are informed in order to apply the above.

On-going monitoring is an essential aspect of effective KYC procedures. The Company can only effectively control and reduce the risk if it has an understanding of normal and reasonable account activity of its customers so that it has means of identifying transactions which fall outside the regular pattern of an account's activity.

Without such knowledge, it is likely to fail in its duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so. Extend of the monitoring needs to be risk-sensitive.

As is abovementioned the company has a full understanding of normal and reasonable account activity of its Clients 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, thus the company implement the Dormant and inactive account monitoring procedure, where on a daily basis monitors Inactive and dormant account to identify any sudden activities without a plausible explanation (e.g. large cash deposits that are suddenly wired out) and that due diligence procedure are established to investigate those sudden client's activities.

### **6.3 Risk Based Approach (RBA)**

The company applies a 'Risk Based Approach'; that is, an approach that not only takes into consideration regulatory and/or legislative matters such as client identification, record keeping and reporting requirements but also assess the nature of their business.

The Company shall develop an in-house automated AML monitoring system to identify any transactions falling outside the regular pattern of each Clients' economic profile through the on-going monitoring of Clients' transactions and activities. Furthermore, the automated monitoring system shall identify all missing information from existing Clients in relation to their economic profiles and any unregular trading patterns.

Execution of withdrawal requests should take place after the POI and POR are checked and are up to date. This should be checked by Finance Department.

Compliance Department should also monitor that the Withdrawal requests have been executed within the requested timeframe;

Deposits should take place after the POI; POR are checked and are up-to-date.

All communication (telephone calls, emails) with the client shall be checked daily by the Qualitative Assurance Department;

Significant deviations are investigated and when a suspicious activity is recognized, further investigation is required in order to obtain explanation 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.

Besides the checks that are done on an ongoing basis by the MLRO, the personnel must report to MLRO any suspicious activity or transaction in order to be reviewed and reported to DAML if it is needed.

## **6.4 Record Keeping**

### **6.4.1 General Guidelines**

The Company must retain:

- copies of, or references to, the evidence they obtained of a customer's identity, for five years after the end of the customer relationship
- details of actions taken in respect of internal and external suspicion reports
- details of information considered by the nominated officer in respect of an internal report where no external report is made

The Company is not required to keep records of the transactions which occurred as part of the business relation, after the business relationship has come to an end, for more than ten (10) years.

Once the period of five (5), or, if applicable, ten (10) years has expired, the Company must delete any personal data relating to CDD and client transactions unless:

- a) the Company is required to retain records containing personal data
  - (i) by or under any enactment, or
  - (ii) for the purposes of any court proceedings;
- b) the data subject has given consent to the retention of that data; or
- c) the relevant person has reasonable grounds for believing that records containing the personal data need to be retained for the purpose of legal proceedings.

### **6.4.2 Records**

The objective is to ensure that a firm meets its obligations and that, in so far as is practicable, in any subsequent investigation the firm can provide the authorities with its section of the audit trail.

#### **➤ Customer Information**

In relation to the evidence of a customer's identity, firms must keep a copy of any documents or information it obtained to satisfy the CDD measures required under the ML Regulations. Some documents which may be used for evidence of identification are more sensitive than others (for example, Armed Forces Cards and Firearms certificates), and firms should deal with such evidence with care.

A firm may often hold additional information in respect of a customer obtained for the purposes of enhanced customer due diligence or ongoing monitoring.

Records of identification evidence must be kept for a period of five years after the business relationship with the customer has ended, i.e. the closing of the account or accounts.

Upon the expiry of the five (5) year period, firms must delete any personal data unless:

- the firm is required to retain records containing personal data by, or under, any enactment, or for the purposes of any court proceedings; or
- the firm has reasonable grounds for believing that records containing the personal data need to be retained for the purpose of legal proceedings; or
- the data subject has given consent to the retention of that data.

A firm which is relied on by another firm for the purposes of customer due diligence must keep the

TDcryptotrade Services LTD is regulated as International Brokerage and Clearing House by M.I.S.A. under license number T2023327 Registered Address: Bonovo Road, Fomboni, Island of Moheli, Comoros Union

records referred to the first paragraph of this section for five years from the ending of the business relationship with the customer.

When an introducing branch or subsidiary undertaking ceases to trade or have a business relationship with a customer, as long as his relationship with other group members continues, particular care needs to be taken to retain, or hand over, the appropriate customer records. Similar arrangements need to be made if a company holding relevant records ceases to be part of the group. This will also be an issue if the record keeping has been delegated to a third party.

#### ➤ **Transactions**

All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the firm's records. Transaction records in support of entries in the accounts, in whatever form they are used, e.g. credit/debit slips, cheques, should be maintained in a form from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect account or customer.

Records of all transactions relating to a customer must be retained for a period of five years from:

- where the records relate to an occasional transaction, the date when the transaction is completed; or
- in other cases, the date the business relationship ended, i.e. the closing of the account or accounts.

But a firm is not required to retain records relating to transactions occurring in a business transaction relationship for more than 10 years.

Upon the expiry of five (5), or, if applicable, ten (10) years firms must delete any personal data unless:

- the firm is required to retain records containing personal data by, or under, any enactment, or for the purposes of any court proceedings; or
- the firm has reasonable grounds for believing that records containing the personal data need to be retained for the purpose of legal proceedings; or
- the data subject has given consent to the retention of that data

#### **6.4.3 Sanctions and penalties**

Where the record keeping obligations under the ML Regulations are not observed, a firm or person is open to prosecution, including imprisonment and/or a fine, or regulatory censure.

## **7 Recognition & Reporting of Suspicious Transactions/ Activities to DAML**

### **7.1 Requirements**

The Company, in cases where there is an attempt of executing transactions which it knows or suspects that are related to money laundering or terrorist financing, reports, through the MLRO its suspicion to the DAML.

### **7.2 Definition**

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

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

- 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.;
- If, as a result of the evaluation described above, the MLRO decides to disclose this information to the DAML, then he prepares a written report, which he submits to the DAML.

### **7.3 Internal reporting**

Any suspicions or knowledge of money laundering must be reported through the internal reporting procedures to the MLRO. The obligation to report to the nominated officer within the firm where they have grounds for knowledge or suspicion of money laundering or terrorist financing is placed on all relevant employees in the regulated sector. All financial sector firms therefore need to ensure that all relevant employees know who they should report suspicions to.

Reporting a suspicion is a defence to a claim for breach of a confidence. Any statements to the press or other publicity must be routed through the MLRO or his deputy. Similarly, any requests for information or statements should be referred to him or his deputy for reply. Confidentiality whilst an investigation is ongoing is of the utmost importance and employees are reminded of the offence of 'tipping-off' which carries the penalties of imprisonment or fine or both.

### **7.4 External reporting**

Any internal report must be considered by the MLRO as soon as reasonably practicable. The MLRO will carry out an investigation of each suspicion report to enable a decision to be made as to whether there are reasonable grounds for the suspicion.

The MLRO must report to the DAML any transaction or activity that, after his evaluation, he knows or suspects, or has reasonable grounds to know or suspect, may be linked to money laundering or terrorist financing, or to attempted money laundering or terrorist financing. Such reports must be made as soon as is reasonably practicable after the information comes to him.

Where there is a suspicion of money laundering and an instruction is received from a client to carry out a transaction or other activity, the MLRO will seek consent from DAML to proceed with the transaction or activity.

The MLRO who reports suspicions of money laundering or terrorist financing internally or to the DAML, is protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions.

## **8 Employees' Obligations, Education and Training**

### **8.1 Requirements**

The Firm must take appropriate measures so that all relevant employees are made aware of the law relating to money laundering and terrorist financing and to the requirements of data protection, and regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.

The MLRO must take reasonable steps to ensure that staff who handle, or are managerially responsible for the handling of, transactions which may involve money laundering are aware of:

- their responsibilities under the Firm's arrangements for the prevention of money laundering and terrorist financing, including those for obtaining sufficient evidence of identity, recognising and reporting knowledge or suspicion of money laundering or terrorist financing
- the identity and responsibilities of the MLRO; and
- the potential effect, on the Firm, on its employees personally and its clients, of any breach of that law.

The MLRO must take reasonable care to provide appropriate anti-money laundering training for its staff who handle, or are managerially responsible for the handling of, transactions which may involve money laundering in order to be aware of:

- the criminal law relating to money laundering and terrorist financing;
- the Law;
- industry guidance;
- the risks money laundering and terrorist financing pose to the business;
- the vulnerabilities of the Firm's products and services; and
- the Firm's policies and procedures in relation to the prevention of money laundering and terrorist financing.

### **8.2 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;
- (c) According to the Law, the Company's employees shall fulfil their legal obligation to report their suspicions regarding Money Laundering and Terrorist Financing, after their compliance with point (b) above.

### **8.3 Training**

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

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 Country.

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.

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.

### **8.4 MLRO Education and Training Program**

The *Senior Management* of the Company shall be responsible for the MLRO of the Company to attend external training. Based on his/her training, the MLRO will then provide training to the employees of the Company further to Section 8.3 above.

The main purpose of the MLRO training is to ensure that relevant employee(s) become aware of:

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