**GUAVAPAY UAB**

**Anti Money Laundering and Counter Terrorism Financing Procedure**

**1. Definitions**

*For the purposes of this Manual, unless the context shall prescribe otherwise:*

Beneficial Owner - means the natural person or natural persons, who ultimately own or control the Customer 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 who ultimately owns or controls a legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that person, including through bearer shareholdings, or through control via other means. Direct ownership is a manner of exercising control whereby a natural person holds a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company. Indirect ownership is a manner of exercising control whereby a company which is under the control of a natural person holds or multiple companies which are under the control of the same natural person hold a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company;

\* The natural person or natural persons, who otherwise exercise control over the management of a legal entity.

b) In the case of a trust, civil law partnership, community or legal arrangement, the Beneficial Owner is the natural person who ultimately controls the association via direct or indirect ownership or otherwise and is such associations’:

\* Settlor or person who has handed over property to the asset pool;

\* Trustee or manager or possessor of the property;

\* Person ensuring and controlling the preservation of property, where such person has been appointed, or

\* The beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates.

Business Relationship - means a relationship that is established upon conclusion of a long-term contract by the Company in economic and professional activities for the purpose of provision of a service, or that is not based on a long-term contract, but whereby a certain duration could be reasonably expected at the time of establishment of the contact.

Customer - means any legal or natural person aiming to conclude a Business Relationship.

Company - means GUAVAPAY UAB, which is incorporated in the Lithuanian Republic with registration number 304642119.

Electronic Verification - performed by third party service provider.

Manual - means the Company’s Prevention of Money Laundering & Terrorist Financing Manual (this Manual).

Money Laundering and Terrorist Financing - Money laundering is the concealment of the illegal origins of income from certain criminal activities, referred to as prior criminal offenses. The scope of terrorist financing is more difficult to define than money laundering. It is understood to be providing assets (including legal assets) for the perpetration of a terrorist act.

Politically Exposed Persons (PEPs) - means the natural persons, who are or have been entrusted with prominent public functions and their immediate family members or persons known to be close associate of such persons (see also section 6.1.4.2. of the Manual).

Shell Bank – a credit institution that has their management, personnel or of financial service provision location situated outside the State of incorporation with no bodies responsible for monitoring of their activities. A shell bank also means a person that provides services similar to those of a credit institution or performs transfers by clearing upon assignment of a third party, with no bodies responsible for their monitoring and control, unless such transfers are effected by electronic money bodies or between the commercial companies that belong to the same group within the meaning of the Financial Conglomerates Law, or between the commercial companies with the same Ultimate Beneficiary.

Suspicious Transaction – means any information, suspicion or reasonable grounds to suspect that the asset, which is subject to the transactions carried out or attempted to be carried out within or through the obliged parties, has been acquired through illegal ways or used for illegal purposes and is used, in this scope, for terrorist activities or by terrorist organizations, terrorists or those who finance terrorism.

**2. Introduction**

GUAVAPAY UAB offers a services platform through guavapay.eu ("GUAVAPAY") that allows people to buy, sell and exchange cryptocurrencies, including math-based currencies such as bitcoin and litecoin. GUAVAPAY also offers, through the service, a platform that allows people to deposit or withdraw funds to and from an account via bank wire transfer, deposit funds to an account payments cards or direct transfer from third party cryptocurrencies exchanges. On GUAVAPAY a Customer can buy or sell cryptocurrencies against a fiat using deposited funds or hold funds indefinitely.

The Company will enforce a strict AML policy with zero tolerance for money laundering activities. We define a money laundering as any activity that is carried out in an attempt to misrepresent the source of funds actually acquired through illegal processes as funds that were acquired through lawful sources/activities.

Money Laundering is the process of disguising the origin of the proceeds of crime. Terrorist Financing provides funds for terrorist activities. The use of services by money launderers and terrorists exposes the Company to significant criminal, regulatory and reputational risk.

This Manual is designed to provide direction to staff on the approach and management of Anti-Money Laundering (AML) and Counter -Terrorist Financing (CTF) within the Company. Additionally, it supports management's objective of mitigation the following risks:

* Money Laundering;
* Terrorist Financing;
* Sanctions;
* Politically exposed persons (PEPs);
* Legal and regulatory risk.

The Company will implement a range of filtration operations for swift and accurate identification of any financial activities that may constitute or are related to money laundering. This will help reduce potential money laundering activities throughout the Company's system.

The CEO must approve all amendments and / or changes of the Manual.

The Manual shall be communicated by the CO to all the employees of the Company that manage, monitor or control in any way the Customers’ transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined herein.

Any questions regarding the Manual should be addressed to the CO or CEO.

When Company’s personnel becomes aware of breaches of law, internal and or external regulations including this Manual, in relation to Money Launder and Terrorist Financing they should immediately bring this to the attention of the CO.

The Manual applies to all types of services offered by the Company.

In this respect, the CO shall be responsible to update the Manual to comply with EU legislation future requirements, as applicable, regarding the Customer identification and due diligence procedures, which we must follow.

**3. Responsibilities of the Management of Company**

The responsibilities of the CEO in relation to the prevention of Money Laundering and Terrorist Financing include the following:

a) To determine, record and approve the general policy principles of the Company in relation to the prevention of Money Laundering and Terrorist Financing and communicate them to the CO;

b) To appoint the CO and, where necessary, it’s assistant, and determine their duties and responsibilities, which are recorded in this Manual;

c) To approve the Manual and ensure that it is communicated to all Company’s employees, who manage, monitor or control in any way the Customer’ transactions as well as have the responsibility for the application and implementation of any and all practices, measures, procedures and controls that have been determined for the prevention of Money Laundering and Terrorist Financing;

d) To ensure that all requirements of the relevant EU Regulations are applied, and assure that appropriate, effective and sufficient systems and controls are introduced for achieving the above mentioned requirement;

e) To assure that the CO and his assistants or any other person, who has been assigned with the duty of implementing the procedures for the prevention of Money Laundering and Terrorist Financing, have complete and timely access to all data and information concerning Customers’ identity, transactions’ documents and other relevant files and information maintained by the Company so as to be fully facilitated in the effective execution of their duties;

f) To ensure that all employees are aware of the person, who has been assigned the duties of the CO, as well as his assistants, to whom they report according to this Manual any information concerning transactions and activities, for which they have knowledge or suspicion that might be related to Money Laundering and Terrorist Financing;

g) To establish a clear and quick reporting chain based on which information regarding Suspicious Transactions is passed without delay to the CO, either directly or through his assistants, if any, and notifies accordingly the CO for its explicit prescription in the Manual;

h) To ensure that the CO has sufficient resources for the effective discharge of his duties;

I) To meet and decide the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected in the internal auditor’s report.

**4. Money Laundering Compliance Officer (MLRO)**

MLRO shall lead the Company’s Money Laundering Compliance procedures and processes and report to the Senior Management. The MLRO shall also have the resources, expertise as well as access to all relevant information necessary to perform his duties adequately and efficiently.

Where it is deemed necessary due to the volume and/or the geographic spread of the services/activities, assistants of the compliance officer are appointed, by geographical district or otherwise for the purpose of assisting the compliance officer and passing internal suspicion reports to him.

In performing his part, the MLRO takes into account the nature, scale and complexity of its business, and the nature and range of the services and activities undertaken in the course of that business.

During the execution of his duties and the control of the compliance of the Company with the Law and the Directive as amended from time to time, the MLRO shall obtain and utilize data, information and reports issued by international organizations, as these are stated in this Manual.

a) The duties of the MLRO shall include, inter alia, the following:

* Designs of measures, procedures and controls:
* To design, based on the general policy principles of the Company, the internal practice, 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 of each department that is involved in the above mentioned. Measures and procedures for the prevention of the abuse of new technologies and systems providing services, for the purpose of Money Laundering and Terrorist Financing. Measures so that the risk of Money Laundering and Terrorist Financing is appropriately considered and managed in the course of daily activities of the Company with regard to the development of new products and possible changes in the Company’s economic profile (e.g. penetration into new markets).

b) Development and establishment of Customers acceptance policy and risk management:

* To develop and establish the Customer Acceptance Policy according to this Manual and KYC (Know Your Customer) Policy and submit it to the CEO 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 CEO for their approval.

c) Monitoring:

* To monitor and assess the correct and effective implementation of the Company's policies, the practices, measures, procedures and controls of point (a) above. In this respect, the MLRO shall apply appropriate monitoring mechanisms, which will provide him with all the necessary information for assessing the level of compliance of the employees of the Company with the procedures and controls, which are in force. In the event that the MLRO 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 CEO.

d) Internal reporting procedures:

* To receive information from the Company’s employees, which could be considered as suspicious of Money Laundering and Terrorist Financing activities or might be related with such activities. The information is received in a written report form (hereinafter the “Internal Suspicion Report”), a specimen of such report is attached in Appendix 1 of the Manual;
* To evaluate and examine the information received as per first point in this section, by reference to other relevant information and discuss the circumstances of the case with the informer. The evaluation of the information of the first point in this section shall be done on a report (hereinafter the “Internal Evaluation Report”), a specimen of such report is attached in Appendix 2 of the Manual;
* If following the evaluation described in the second point, the MLRO decides to notify the Unit for Combating Money Laundering (FNTT), then he should complete a written report and submit it to the FIU the soonest possible. A template of such report (hereinafter the “MLRO Report to the FNTT”), is attached in Appendix 3 of the Manual;

After the submission of the report to the FNTT, the account involved and any other connected accounts, are closely monitored by the MLRO and following any directions from the FNTT, thoroughly investigates and examines all the transactions of the accounts;

* If following the evaluation described in the third point the MLRO decides not to notify the FNTT then he should fully explain the reasons for such a decision;
* To act as a first person of contact with the FNTT, upon commencement of and during an investigation after of filing a report to the FNTT.

e) Preparation of Customers’ list:

* To ensure the preparation and maintenance of the lists of Clients categorized following a risk based approach, which contains, among others:

• The names of Customers,

• Their account number and,

• The dates of the commencement of the Business Relationship.

 Moreover, the MLRO ensures the updating of the said list with all new or existing Customers, if will be obtained any additional information.

f) Detection, recording and evaluation of risks and updating of procedures:

* To detect, record, and evaluate, at least on an annual basis, all risks arising from existing and new Customers, new services and update and amend the systems and procedures applied by the Company for the effective management of the aforesaid risks;
* Evaluate the systems and procedures applied by a third person, on whom the Company relies for Customers identification;
* To obtain and utilize date, infrastructure and results issued by the relevant International Organisations (i.e. FATF, Moneyval, UN and others);
* To ensure that the duties of the MLRO assistants been done and controlled.

g) Training:

* To provide advice and guidance to the 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 and Terrorist Financing as applicable and relevant to the services being offered by the Company;
* To determine whether the Company's employees need further training and education for the purpose of preventing Money Laundering and Terrorist Financing and organizes appropriate training sessions/seminars.

h) Reporting:

* To respond to all requests and queries from the FNTT, provide all requested information and fully cooperate with the FNTT.

i) Maintenance of registry:

* To maintain an internal registry, which includes the reports of suspicions of Money Laundering and Terrorist Financing activities by the Company's employees and decisions to inform or not about these suspicions to FNTT.

**5. Internal Auditor Obligations**

The AML Compliance Officer will identify an independent third party that is primarily focused on AML compliance matters, or other qualified independent third party to conduct the testing on an annual basis. The AML Compliance Officer, Manager, or other AML compliance personnel shall not conduct the independent audit.

GUAVAPAY will periodically subject its compliance program to the thorough scrutiny of a qualified independent reviewer at least once a year, and also upon the change of any significant business function. The final report is reviewed by the MLRO, who is responsible for ensuring that corrective measures are swiftly and effectively implemented. An independent review will be conducted to audit the Company's process, procedures and results for the prior period. Each of these reviews could potentially result in the identification of unreported suspicious activity. If suspicious activity is identified through these reviews, the MLRO is responsible for further investigation and subsequent SAR (Suspicious Activity Report) reporting.

The following obligations of the internal auditor are addressed specifically for the prevention of Money Laundering and Terrorist Financing:

a) To review and evaluate the scope of the testing to be performed with regards to the procedures and controls for the prevention of Money Laundering and Terrorist Financing;

b) The findings and observations shall be submitted, in a written report form, which the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected, including an implementation schedule and time-frame for implementation;

c) The internal auditor shall be responsible for reviewing the adequate implementation of a risk-based approach by the Company, at least annually.

The report on the results of the inspection concerning the compliance with the measures for prevention of Money Laundering and Terrorist Financing shall set out the following information:

* Date of the inspection;
* Name and position of the person conducting the inspection;
* Purpose and description of the inspection;
* Evaluation of the overall integrity and effectiveness of the Company's AML procedure;
* Reviewing of the flow of funds and the scope of GUAVAPAY business to determine whether additional compliance controls should be added to the AML procedure;
* Reviewing and testing of a compliance for record keeping and record retention policies;
* Inspection’s results;
* If the inspection reveals any deficiencies in the procedures or their implementation, the report shall set out the measures to be applied to remedy the deficiencies and respective time schedule and the time of a follow-up inspection;
* If a follow-up inspection is carried out, the results of it shall be added to the inspection report, which shall state the list of measures to remedy any deficiencies discovered in the course of the follow-up inspection, and the time actually spent on remedying the same;
* The inspection report shall be presented to the CO, who shall decide on taking measures to remedy any deficiencies discovered.

Records of independent testing must be retained by the CO for at least five years.

**6. Risk-Based Approach**

*6.1. General Policy*

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

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

*6.2. Risk-based approach adopted*

The Company follows to the adopted risk-based approach with following general characteristics:

* Recognizing that the Money Laundering or Terrorist Financing threat varies across Customers, countries and services;
* A creating of more cost-effective system;
* Prioritization in effort and actions of the Company in response to the likelihood of Money Laundering and Terrorist Financing occurring through the use of the services.

*6.3. Specific Measures*

This approach involves specific measures and procedures in assessing the most cost effective and appropriate way to identify and manage the Money Laundering and Terrorist Financing risks faced by the Company. Such measures include:

* Identifying and assessing the Money Laundering and Terrorist Financing risks emanating from particular Customers, services, and geographical areas of operation;
* Managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls;
* Continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

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

* Geographical location;
* The nature and economic profile of Customers;
* The volume and size of transactions;
* The degree of risk associated with each area of services;
* The country of origin and destination of Customers’ funds;
* Deviations from the anticipated level of transactions;
* The nature of business transactions.

The MLRO is responsible for the development of the policies, procedures and controls on a risk-based approach. Further, the MLRO is responsible for the implementation of the policies, procedures and controls on a risk-based approach.

The Company allows to the Customers to deposit using Bank Wires and Credit Cards. Throughout the ongoing procedures the Company monitors the risks entailed via these deposit methods.

The procedure, which the MLRO Department use to inspect the Customers’ accounts on an ongoing basis, is applied to all Company’s active Customers, depending on their risk categorization. To the ensuring of proper and effective monitoring of Customers transactions the Company applies adequate and appropriate systems and procedure. The Company uses the procedure to inspect the Customers’ transactions on an ongoing basis of the monitoring of the actual versus the initial set level of transactions per the pre-set economic profile data of Customers, constructed during the establishment of the Business Relationship.

***6.4. Identification of Risks***

6.4.1. General/Principles

The risk-based approach involves the identification, recording and evaluation of the risks and it’s have to be managed. The Company shall assess and evaluate the risks it faces for prevention of Money Laundering or Terrorist Financing. The particular circumstances of the Company determine the suitable procedures and measures that need to be applied to counter and manage risk.

The Company shall, at all times, be in a position to demonstrate that the extent of measures and control procedures it applies, are proportionate to the risk it faces.

6.4.2. Company Risks

The following are sources of risks which the Company faces with respect to Money Laundering and Terrorist Financing:

a) Risks based on the Customer's nature:

* A Customer’s unwillingness to provide information required for identification and verification.
* Complexity of ownership structure of legal persons;
* Companies with bearer shares;
* Companies incorporated in offshore centers;
* PEPs;
* Customers engaged in transactions which involve significant amounts of fiat;
* Clients from high risk countries or countries known for high level of corruption or organized
* crime or drug trafficking.

b) Risks based on the Customer’s behavior:

* Customers transactions where there is no apparent legal financial/commercial rationale;
* Situations where the origin of wealth and/or source of funds cannot be easily verified;
* Unwillingness of Customers to provide information on the Beneficial Owners of a legal person.

c) Risks based on the Company’s services (for deposit/withdrawal by cryptocurrencies, when determining the ownership of an e-wallet to a Customer is complicated):

* Transactions which may favor anonymity;
* Services that allow payments to third persons.

***6.5. Design and Implementation of Measures and Procedures to Manage and Mitigate the Risks***

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

* Determination of the categories of low or high risk Customers, which includes the Customers prescribed in this Manual and KYC procedure;
* Adaption of the Customer Due Diligence Procedures in respect of Customers, in line with their assessed Money Laundering and Terrorist Financing risk;
* Requiring the quality and extent of required identification data for each type of Customer to be of a certain standard (e.g. documents from independent and reliable sources, third person information, documentary evidence);
* Obtaining additional data and information from the Customers, where it 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;
* Conducting ongoing monitoring of the Business Relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the Customer, 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;
* Ongoing monitoring of high risk Customers’ transactions and activities.

Documenting the measures and procedures set out in this section will assist the Company to prove:

a) The ways used to identify, record and assess the risk of its services being used for Money Laundering or Terrorist Financing;

b) Determination of the introduction and implementation of specific measures and procedures for the management and mitigation of risks; and

c) The methods applied for monitoring and improving, whenever deemed necessary, the specific measures, procedures and controls.

***6.6. 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. Customers’ activities change. The same happens to the financial instruments and the transactions used for Money Laundering and Terrorist Financing.

In this respect, it is the duty of the CO to undertake regular reviews of the characteristics of existing Customers, new Customers, services, the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics.

***6.7. Relevant International Organizations***

For the development and implementation of appropriate measures and procedures on a risk based approach, and for the implementation of Customer Identification and Due Diligence Procedures, the CO shall consult data, information and reports that are published in following relevant international organizations:

a) FATF - [www.fatf-gafi.org](http://www.fatf-gafi.org/)

b) The Council of Europe Select Committee of Experts on the Evaluation of Anti¬-Money

Laundering Measures (hereinafter “MONEYVAL”) - [www.coe.int/moneyval](http://www.coe.int/moneyval)

c) The International Money Laundering Information Network (IMOLIN) - [www.imolin.org](http://www.imolin.org/)

d) The UN Security Council Sanctions Committees <https://www.un.org/securitycouncil/sanctions/information>

e) EU Common legislation <https://europa.eu/european-union/index_en>

f) Lithuanian legislation

g) Any and all sources that are used for screening by Compliance Companies (i.e. Accuity, WorldCompliance, Worldcheck, etc.) of the Company’s Customers as a standard procedure.

**7. Customers’ Acceptance Policy**

The procedures described herein shall apply to the EEA and third country (non-EEA) Customers, in which the Company has a right to provide it services.

A clear Customer Acceptance Policy (hereinafter the “CAP”) is developed and established completely in line with the provisions of the Law and the Directive. The CAP defines the criteria for accepting new Customers, including non-acceptable Customers, and defines the Customer categorization criteria (low risk, medium risk and high risk), which shall be apply by the Company's employees (which shall be involved in the Customer Account Opening process).

The Company and or the Company’s employees shall take into consideration (for the non-acceptance of clients and the categorization into low, medium and high risk clients) factors such as the Customer’s background, type and nature of his business activities, country of residence, the services, the anticipated level and nature of business transaction as well as the expected source and origin of funds. The CAP procedure set out the instructions in relation to the Customers’ accounts from registering and opening an account with the Company until the time of closing/terminating of that account.

 The CO shall be responsible for applying all the provisions of the CAP. In this respect, the Compliance and Customer Service Departments shall also be assisting the CO with the implementation of the CAP, as applicable.

***7.1. Criteria for Accepting of New Customers***

This Section describes the criteria for accepting new Customers, based on their risk categorization. The level of due diligence required, when considering anti-money laundering procedures within the Company, should take a risk-based approach. This means the amount of resources spent in conducting due diligence in any one relationship that is subject of risk should be in proportion to the magnitude of the risk that is posed by that relationship. This section defines the risk assessment methodology for the initial risk categorization of Customers and also for ongoing monitoring.

According to EU legislation and Lithuanian local law in the process of opening an account the following procedures will take place:

* Establishment of the Customer’s identity

a) For physical person:

* a collection of personal details, including first / last name, full address, telephone number, e-mail, country of residence;
* verification of identity through an acceptable ID document and proof of residence document that issued by an independent and reliable source. It is never acceptable to use the same verification data or information for verifying the Customer’s identity and verifying its home address;

b) For legal entity

* name of the Company, registration number and country of establishment, residential and business address, contact details (telephone, fax, e-mail, website), business activity, information about Beneficial Owner, directors and representatives, confirmation of source of funds;
* identifying the Beneficial Owner and taking reasonable measures to verify that person's identity so that the Company is satisfied that it knows who the Beneficial Owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the Customer. The Company shall also verify any person purporting to act on behalf of the Customer is so authorised and identify and verify the identity of that person;
	+ E-mail verification;
	+ Filling of questionnaire form;
	+ Assessing and, as appropriate, obtaining information on the purpose and intended nature of the Business Relationship.

The Company chooses additional due diligence measures in order to manage and mitigate an established risk of Money Laundering and Terrorist Financing that is higher than usual. To perform these duties the Company may, among other things, apply one or several of the following due diligence measures:

* Verification of information additionally submitted upon identification of the person based on additional documents, data or information originating from a credible and independent source;
* Gathering additional information on the purpose and nature of the Business Relationship and verifying the submitted information based on additional documents, data or information that originates from a reliable and independent source;
* Gathering additional information and documents for the purpose of identifying the source and origin of the funds;
* Verification of the data contained in the documents presented to the Company by Legal Entities against the information contained in the European Business Register databases;
* Receiving permission from the senior management to establish a Business Relationship.

Upon application of Enhanced Due Diligence measures, the Company must apply the monitoring of a Business Relationship more frequently than usually, including reassess the Customer’s risk profile not later than six months after the establishment of the Business Relationship.

All documents and data must be collected before accepting a new Customer. Pursuant to Law on the prevention of money laundering and terrorist financing, 19 June 1997 No. VIII-275, of Lithuanian Republic, we do not accept any anonymous or fictitious accounts.

An account will be opened only after the relevant pre-account opening due diligence and identification measures and procedures have been conducted, according to the Company's principles and internal procedures.

Categories below, take into consideration factors such as the Customer’s background, residency, type and nature of its business activities (including involvement in public contracts), the services, the anticipated level and nature of business transactions as well as the expected source and origin of funds.

***7.1.1. Beneficial Owner (BO)***

In cases of Legal Entities:

* The natural person who ultimately owns or controls a legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that person, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Union law or subject to equivalent international standards which ensure adequate transparency of ownership information;
* BO can has:

a) a direct ownership that means a manner of exercising control whereby a natural person holds a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company;

b) indirect ownership that means a manner of exercising control whereby a company which is under the control of a natural person holds or multiple companies which are under the control of the same natural person hold a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company.

After all possible means of identification have been exhausted and BO cannot be identified and there is no doubt that such person exists or where there are doubts as to whether the identified person is a BO the natural person who holds the position of a senior managing official is deemed as a Beneficial Owner.

The Company registers and keeps records of all actions taken in order to identify the Beneficial Owner.

In the case of a trust, civil law partnership, community or legal arrangement, the Company considers a natural person who ultimately controls the association via direct or indirect ownership or otherwise as a Beneficial Owner, and could be:

a) Settlor or person who has handed over property to the asset pool;

b) Trustee or manager or possessor of the property;

c) Person ensuring and controlling the preservation of property, where such person has been appointed;

d) The beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates;

e) The CEO may be designated as a Beneficial Owner.

***7.1.2. Low Risk Customers***

Pursuant to Directive (EU) 2018/843 and “Law on the prevention of money laundering and terrorist financing, 19 June 1997 No. VIII-275, of Lithuanian Republic” the Company can applies Simplified Due Diligence measures to Customers before establishment of a Business Relationship. Before applying simplified Customer due diligence measures, we shall ascertain that the Business Relationship or/and the transaction presents a lower degree of risk. In cases of the application of Simplified Due Diligence measures we ensure sufficient monitoring of transactions and Business Relationships.

In the cases of low risk Customers the Company applies the simplified Customer identification and request minimal information about a Customer (only necessary information to verification).

It shall be noted that, where a Customer Legal Entity is a non-face-to-face Customer, it cannot be considered “low risk” by the definition within the law, and the Simplified Due Diligence procedure should not be applied.

**7.1.3. Medium Risk Customer**

The Company shall accept Customers who are categorized as medium risk Customers as long as the general principles under Section 6.1 of the Manual are followed. For this category additionally, the Customers must proof their residence addresses.

***7.1.4. High Risk Customers***

7.1.4.1. The Company applies Enhanced Due Diligence measures in order to adequately manage and mitigate a higher-than-usual risk of Money Laundering and Terrorist Financing. Enhanced Due Diligence measures are applied always when:

a) Upon identification of a person or verification of submitted information, there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the Beneficial Owner;

b) The Customer is a Politically Exposed Person, their family member or a close associate, if there are no other factors that refer to a higher-than-usual risk;

c) The Customer is from a high-risk third country or their place of residence or seat or the seat of the payment service provider of the payee is in a high-risk third country;

d) The Customers are from such country or territory or their place of residence or seat or the seat of the payment service provider of the payee is in a country or territory that, according to credible sources such as mutual evaluations, reports or published follow-up reports, has not established effective AML/CFT systems that are in accordance with the recommendations of the Financial Action Task Force (FATF);

e) Any other Customer determined and classified by the Company with a higher risk level of Money Laundering or Terrorist Financing;

f) Entities whose primary business involves electronic gambling.

Upon assessment of factors referring to a higher risk the following is deemed a situation increasing risks related to the Customer as a person:

a) The Business Relationship foundations based on unusual factors, including in the event of complex and unusually large transactions and unusual transaction patterns that do not have a reasonable, clear economic or lawful purpose or that are not characteristic of the given business specifics;

b) The Customer is a resident of a higher-risk geographic area listed below:

* + That, according to credible sources such as mutual evaluations, detailed evaluation reports or published follow-up reports, has not established effective AML/CFT systems;
	+ That, according to credible sources, has significant levels of corruption or other criminal activity;
	+ That is subject to sanctions, embargo or similar measures issued by, for example, the European Union or the United Nations;
	+ That provides funding or support for terrorist activities, or that has designated terrorist organizations operating within their country, as identified by the European Union or the United Nations.

c) The Customer is a legal person or a legal arrangement, which is engaged in holding personal asset

d) The ownership structure of the Customer company appears unusual or excessively complex, given the nature of the company’s business;

7.1.4.2. PEP (Politically Exposed Person)

The Company shall apply the strengthened due diligence measures, when establishing a Business Relationship and executing a transaction with:

* A Politically Exposed Person (as an individual or Beneficial Owner) from another EEA member state or a third country; or
* At least within 12 months after a Politically Exposed Person no longer performs important public functions placed upon them (ex-PEP).

In these cases, additional we request:

a) Title of position in the entity (for legal entities);

b) Current or former political title(s) or position(s);

c) Length of time in the political title(s) or position(s), including dates served in each title or position;

d) Where applicable in the case of immediate family members or close associates of PEPs/ex-PEP, the nature of the relationship to the PEP;

e) Applies measures to establish the origin of the wealth of the person and the sources of the funds that are used in the Business Relationship (e.g. wage statements, interest statements, tax returns, bank statements), the clear description of the main business/professional activities/operations, generating funds for the said person);

f) All PEPs are required to fill the form in Appendix 6 and supply proof of funds and evidence of wealth.

The meaning PEP includes the following natural persons who are or have been entrusted with prominent public functions’ in a foreign country:

* Heads of State, heads of government, ministers and deputy or assistant ministers;
* Members of parliaments;
* 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, chargé d'affaires and high-ranking officers in the armed forces (and other than in respect of relevant positions at Community and international level);
* Members of the administrative, management or supervisory bodies of State-owned enterprises.

These categories do not include middle-ranking or more exercising/discharging their duties at levels lower than national.

For the Customers checking the Company/third party uses a reliable commercial electronic database for PEPs, receives the information from the Customer himself or from publicly available information.

The Company shall pay more attention, when the said persons originate from a country, which is widely known to face problems of bribery, corruption and financial irregularity and whose anti-money laundering laws and regulations are not equivalent with international standards. In order to effectively manage such risks, the Company shall assess the countries of origin of its Customers in order to identify the ones that are more vulnerable to corruption.

In the case of Legal Entities, the procedures will aim at verifying whether the Beneficial Owners, authorized signatories and persons authorised to act on behalf of the Legal Entities constitute PEPs. In case of identifying one of the above as a PEP, then automatically the account of the Legal Entity should be subject to the relevant procedures specified in this section of the Manual.

Before establishing a Business Relationship with a PEP, the Company shall obtain adequate documentation, but also to assess its business reputation.

The CEO of our Company shall decide establishment of a Business Relationship.

Monitoring of the Business Relationship with higher frequency is obligatory. The account shall be subject to annual review in order to determine whether to allow its continuance of operation. A short report shall be prepared summarizing the results of the review by the person who is in charge of monitoring the account. The report shall be submitted for consideration and approval to the CEO and filed in the Customer’s file.

If the PEP is a prior Customer who has had a change in circumstances that leads to the Customer now being a PEP/ex-PEP, he need to pass enhanced due diligence check (to establish the source of wealth and source of funds; to conduct enhanced annual ongoing monitoring of the Business Relationship). If, in during of a Business Relationship with a Customer (natural or legal person), subsequently it is ascertained that the persons involved are or have become PEPs, the CEO should approve or decline of continuing the Business Relationship.

If as part of the yearly review, the PEP does not show cooperation in provision of updated/ missing identification and verification data his account shall be terminated within 15 days from the time the first email was set to the Customer.

PEPs who ceased to hold office over one year ago may be accepted. However, firms should exercise professional judgment in deciding whether any additional due diligence or monitoring might be appropriate.

In addition, this clause applies to:

PEP/ex-PEP family members:

 a) The spouse, or a person considered to be equivalent to a spouse;

 b) A child and their spouse, or a person considered to be equivalent to a spouse;

 c) Parents.

A close associate person:

a) A natural person who is known to be the Beneficial Owner or to have joint Beneficial Ownership of a legal person or a legal arrangement, or any other close business relations;

b) A natural person who has sole Beneficial Ownership of a legal entity or legal arrangement, which, is known, to have been set up for the de facto benefit of PEP/ex-PEP.

7.1.4.3. Factors, which bit reduces the risk for Customers as a Legal Entities

Upon assessment of factors referring to a lower risk is deemed a situation reducing risks relating to the Customer type:

a) The Customer is a company listed on a regulated market, which is subject to disclosure obligations that establish requirements for ensuring sufficient transparency regarding the Beneficial Owner;

b) The Customer is a Legal Person governed by public law established in Lithuania;

c) The Customer is a governmental authority or another authority performing public functions in Lithuania or a contracting state of the European Economic Area;

d) The Customer is an institution of the European Union;

e) The Customer is a credit institution or financial institution acting on its own behalf or a credit institution or financial institution located in a contracting state of the European Economic Area or a commercial electronic database for PEPs, third country, which in its country of location is subject to requirements equal to those established in Directive (EU) 2015/849 of the European Parliament and of the Council and subject to state supervision;

f) A person who is a resident of a country or geographic area having the characteristics specified in clauses a)– d) above mentioned.

Upon assessment of factors referring to a lower risk in accordance with subsection above, at least the following situations where the Customer is from or the Customer’s place of residence or seat is in, may be deemed a factor reducing geographic risks:

a) A contracting state of the European Economic Area;

b) A third country that has effective AML/CFT systems;

c) A third country where, according to credible sources, the level of corruption and other criminal activity is low;

d) A third country where, according to credible sources such as mutual evaluations, reports or published follow-up reports, AML/CFT requirements that are in accordance with the updated recommendations of the Financial Action Task Force (FATF), and where the requirements are effectively implemented.

***7.2. Not Acceptable Customers***

The following list predetermines the type of Customer who are not acceptable for establishing a Business Relationship:

* Customers who fail or refuse to submit, the requisite data and information for the verification of their identity and the creation of their profile, without adequate justification;
* Potential Customers that require to open anonymous account;
* The Customer acts on behalf or upon assignment of a third party, or its activities lead to suppose that the Customer may be a Shell Bank or satisfy the criteria of a Shell Bank;
* Restricted countries;
* Companies whose shares are in bearer form;
* Minors – under the age of 18.

For more information please refer attached hereto as Appendix 4.

***7.3. Account Termination Procedure***

7.3.1. According to our policies, the Company has the right to terminate a relationship with the Customer at any time. If for any reason the Company decides to discontinue providing the service, we will notify the Customer by providing at least a 3 (three) calendar days’ notice (which may be provided by email, facsimile etc.). This clause will be apply on the following occurs (including but not limited):

* If the Company believes that the Customer has breached any of the Company’s policies, including but not limited to engagement in fraudulent, unlawful or improper activity, money laundering activities, or conduct otherwise in violation of Company’s policies;
* Upon an issuance if an application, order, resolution or other announcement in relation to the bankruptcy or winding up proceedings in which Client is involved, immediately without notice;
* The death of the Customer, immediately without notice;
* The Customers who fail or refuse to submit, the requisite data and information for the purpose of completing the Customer Due Diligence, all data and information required for completion of their profile of risk level; within the reasonable time frame;
* If during the Business Relationship and/or as part of updating Customers’ records, they fail or refuse to provide the missing/ updated verification data and information;
* Any client that can be re-categorized as Non-Acceptable following the ongoing account monitoring.

7.3.2. Account Termination due to Fraud or Abuse

If during ongoing account and/or transactions monitoring the Company has identified a Customer engaged in a fraudulent or abusive activity, we shall follow the relevant internal procedures to determine whether account qualifies for closure. If sufficient evidence of abuse/ fraudulent activity is collected, or there are sufficient grounds to believe so, account shall be closed within 15 days from the initial contact or 15 days from the date the case is identified and as part of the account monitoring program for existing Customers, whichever occurs first.

7.3.3. Account Termination of Existing Clients with missing/outdated identification records

If as part of the ongoing monitoring and/or at any point in time it is identified that identification records on the Customer file are outdated (i.e. identification documents, profiling information) the Company immediately contact with the Customer and urge for provision of updated/missing records within the set timeframe.

If the Customers do not show cooperation in provision of updated/ missing information they accounts shall be terminated within 15 business days from the time the first email was sent to them or the first telephone contact was made, whichever occurs first.

The Business Relationship must be terminated within the date of the deadline’s expiry and all deposited funds must immediately be returned to the Customers, in the same payment method in which it’s originated. The procedure for returning the funds must occur regardless of whether the Customers have requested the return of their funds or not.

No funds are withheld and accounts not frozen, except of cases of suspicion of money laundering, where the Company is under obligation to immediately report their suspicion to Financial Intelligence Unit "FNTT". The outcome of the said review shall be recorded in an individual note/form, which shall be kept in the respective Customer file.

***7.4. Dormant Accounts***

The Company has adopted the Dormant Account Policy (attached herein as Appendix 5) under which an account is classified as dormant if it remains inactive or no transactions have been carried out in relation to the account by or on the instructions of the account holder for period of 1 year. If an account is classified as dormant then:

* We may restrict payments in or out of your account to protect against fraud but we will let you know first;
* Our employees will find out reasons of non-operation and will request to Customer to close the account.

The Company’s employees shall be responsible to review at least annually the adherence of the Company with the above.

**8. Customer Due Diligence and Identification Procedures**

The Company’s Customers shall be comprised of both natural persons and legal entities that fulfill the requirements depicted in this CAP procedure. The Company shall duly apply Customer identification procedures and Customer Due Diligence measures, before of establishing a Business Relationship.

Customer identification procedures and Customer Due Diligence measures shall comprise at a minimum of the following:

* Identifying the Customer and verifying the Customer’s identity on the basis of documents, data or information obtained from a reliable and independent source;
* Identifying the Beneficial Owner and taking risk-based and adequate measures to verify the identity on the basis of documents, data or information obtained from a reliable and independent source so that the person carrying on in financial or other business knows who the Beneficial Owner is; as regards Legal Persons, trusts and similar legal arrangements, taking risk based and adequate measures to understand the ownership and control structure of the Customer;
* Obtaining information on the purpose and intended nature of the Business Relationship;
* Obtaining information in regards to anticipated account turnover, the nature of the transactions, the expected origin of incoming funds;
* Information of the Customer’s wealth level;
* To conduct ongoing monitoring of the Business Relationship including analysis of transactions, the business and risk profile, including where necessary, ensuring the relevance of the documents, data or information on the Customer's file.

It is the duty of the Company's responsible employees to apply all the relevant Customer Due Diligence procedures and also are responsible to collect and file of the required documents. Further, the compliance officer shall be responsible to maintain and use Customer Due Diligence procedures per the requirements of the EU Law and the Directive.

Customer Due Diligence requirements shall be applied not only to all new Customers, but also to existing Customers at appropriate times, depending on the level of risk of being involved in Money Laundering or Terrorist Financing.

In addition to the obligation of this Manual and procedures, the Company shall check the adequacy of the data and information of the Customer’s identity and his/her profile, whenever one of the following events or incidents occurs:

* An important transaction takes place which appears to be unusual compared to the normal pattern of transactions and the Customer's profile;
* A material change in the Customer's legal status and situation, such as:

a) Change of directors/secretary

b) Change of registered shareholders and/or Beneficial Owners

c) Change of registered office

d) Change of trustees

e) Change of corporate name and/or trading name

f) Change of the major business activities

* A material change in the way and the rules the Customer’s account operates, such as: changes in the persons that are authorised to operate the account

***8.1. Customers’ Registration Process***

Electronic identity verification is carried out through a third party. Our partner cumulatively satisfy the following conditions:

* Online verification;
* The electronic databases kept by the third party or to which the third party has access are registered to and/or approved by the data protection commissioner in order to safeguard personal data (or the corresponding competent authority in the country the said databases are kept);
* Electronic databases provide access to information referred to both present and past situations showing that the person really exists and providing both positive information (at least the Customer’s full name, address and date of birth) and negative information (e.g. committing of offenses such as identity theft, inclusion in deceased persons records, inclusion in sanctions and restrictive measures’ list by the Council of the European Union and the UN Security Council);
* Electronic databases include a wide range of sources with information from different time periods;
* Storage of the used information and results of a person verification.

The third party establishes mechanisms for the carrying out of quality controls in order to assess the quality of the information on which it relies.

**8.1.1. Natural Persons**

8.1.1.1. The verification of the Customer’ 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.

The Company shall be satisfied that it’s dealing with a real person and shall obtain sufficient evidence of identity to verify that he/she is a person as he/she indicated himself.

In order to create an account in our platform the Customer is requested to provide, inter alia, the following details for the identification:

* First and Last Names
* Personal code ( or date of Birth)
* Nationality
* Contact Details (telephone, email)
* Country of residence (country, city, street, house/building number, postal code)
* Valid passport or ID document (must be an original document, photocopied documents are not acceptable).

After person’s verification and checking on different lists (sanctions, black, PEP and etc.) the Company make available low/basic risk level for the Customer with monthly limits of EUR 1 000 (please see the Company’s KYC procedure).

If a person will be identified as a PEP, hi/she will be obligatory to:

* Pass an Enhanced Due Diligence;
* Fill a questionnaire form;
* Provide an adequate documentation to ascertain not only the identity of the said person, but also to assess his business reputation (e.g. reference letters from third parties);
* In certain cases the company might ask for a clean criminal record letter issued in the PEP’s country of origin.

8.1.1.2. For the increasing of monthly limit the Customer must to pass an additional check:

* To fill questionnaire form with information of the:

a) Taxpayer ID

b) Residence address

c) Information of the revenues/employment status

d) Bank details

e) Purpose of cryptocurrency purchases

f) Information about payment methods

g) Account activity (required a monthly turnover).

* Payment card verification (the Customer must attach selfie where can see his/her name on the front of the card and expiry date, plus show first six and last four digits only; the other numbers have to be hidden by the Customer, before he send to us the card’s copy);
* To proof a residence address with one of the documents – utility bill, tax assessment, bank account statement, rent agreement, bank reference letter; a document must be dated no older than three months;
* To proof a source of funds and wealth (include but not limited salary, bank account statement for the last three months, loan agreement, tax return, financial statement, trade logs, profit or interest, Inheritance or gift, activities, which generated the funds being used in the transaction);
* The Customer’s experience in trading of cryptocurrencies.

8.1.1.3. Declaration

The Customer must tick the following check box if he wishes to apply for the opening of an account with the Company:

□ I agree with the Terms and Conditions and Privacy Policy (hyperlinked to these policies).

After registration, the Customer receive a “welcome email” from the Company, asking him/her to verify e-mail address and using a Two-Factor Authentication procedure.

No deposits are to be accepted by the Company, where the Customer has not passed on a full identification and not completed his/her profile.

Any Customer trying to register with the e-mail address of an existing Customer shall be automatically blocked.

8.1.1.4. The profile information is stored in the Customer file in the Company’s database. The relevant information updated periodically by the Company based on provided information of the Customer, especially those concerning high risk Customers.

**8.1.2. Legal entity**

The Company shall obtain adequate data and information so as to understand the ownership and control structure of the Customer. The Company shall verify the identity of the Beneficial Owners of the Customers’ accounts.

In order to create a corporate account with the Company, the Customer (Legal Entity) is requested to provide, inter alia, the following details about the Legal Entity in order to identify the entity (filling of the questionnaire for Legal Entities):

* Full registered name
* Possible trade name
* Type of company
* Country of incorporation
* Registration number
* Registered address and head/principal office address
* VAT number
* Contact details
* Website address, if applicable
* Financial Information
* The purpose of opening the corporate account
* Principal Activities of the company / Nature of the company / Size of the company’s operations
* Country/-ies of activities of legal entity
* The anticipated account turnover
* The expected origin (source of funds) of incoming funds to be credited in the account
* Company's bank account information

8.1.2.1. The following documents must be obtained in order for the Legal Entity to create a corporate account with the Company:

* Memorandum and Articles of Association
* Certificate of Incorporation
* Recent utility bill to verify business address
* Certificate of Director(s)
* Certificate of Secretary
* Certificate of Shareholder(s)
* Certificate of Good Standing
* Certificate of Incumbency
* Latest audited financial statements (if applicable)
* In the cases where the registered shareholders act as nominees of the Beneficial Owners, a copy of the trust deed/agreement concluded between the nominee shareholder and the Beneficial Owner, by virtue of which the registration of the shares on the nominee shareholder’s name on behalf of the Beneficial Owner has been agreed;
* A resolution of the board of directors of the legal person for the opening of the account and granting authority to those who will operate it;
* Ownership structure and ownership official certificate of shareholders of the group that the Legal Entity may be part of (country of incorporation of the parent company, subsidiary companies, and associate companies, main activities and financial information).

The Company shall take all necessary measures for the full ascertainment of the Legal Entity’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 Entity according to the Company's procedures. Full details and KYC of the representatives/directors/shareholders (over 25%)/authorised signatories/UBOs’/ any individual(s) who otherwise exercise control over the management of the Legal Entity, including but not limited to:

a) Full name

b) Nationality

c) Passport/ID number

d) Date of birth

e) Place of birth

f) Contact information

g) Country of residence

h) Residential address (i.e. street, number, area)

i) Tax Number

j) Financial information

* Ledger of the shareholders
* Credit card copies/credit card statement and/or bank statement
* A signed resolution by the Board of Directors of the legal entity or equivalent document to authorise the opening of an account and conferring authority to those who shall operate it and authorising the use of corporate funds (if applicable)
* Tax declaration and/or Tax letter in order to ensure sufficient documents are obtained for mitigating the risk of tax evasion (recent tax return and/or letter of settlement of tax responsibilities)
* Filled questionnaire form for the Legal Entity.

The process of verification of the identity of the representatives of the Legal Entity shall be the same as the process of other Customers (i.e. - Electronic Verification/ verification via documents and screening against negative databases).

All documents must be recent, issued by the relevant authority and not older than 3 months.

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 registrar of companies or from a corresponding authority in the company’s country of incorporation and/or request information from other sources in order to establish that the applicant company (Legal Entity) is not in the process of being dissolved, or liquidated, or struck off from the registry of the Registrar of Companies.

8.1.2.2. Where any of the director(s) and/or shareholder(s) and/or secretary of the Legal Entity is a Legal Entity as well, the application will be rejected.

The Company’s employees also performs background checks, using data and information obtained from a reliable and independent source for all directors, UBOs’ and the legal entity itself. The information of the company's additional owner shall be collected and stored in the Customer’s file. The Company shall take additional measures to ensure that the Legal Entity operate from the address of their main offices and carry out legitimate activities in all respects.

8.1.2.3. The policy of the Company shall be to allow account access to only one person and not to all persons identified as beneficiaries / holders of the corporate account.

Verification of the identity of a Natural Person that have the right to manage and fund the account occurs during Customer onboarding and is subject to 15 days verification policy if applicable, based on the predefined thresholds, and should be completed before account becomes operational.

8.1.2.4. If any changes occur in the structure or the ownership status or to any details of the Legal Entity, or any suspicions arise emanating from changes in the nature of the transactions performed by it via its account, it is imperative that further inquiries should be made for ascertaining the consequences of these changes on the documentation and information held by the Company and all additional documentation and information for updating of the Legal Entity profile.

8.1.2.5. All information of the Legal Entity is store in the Customer’s file along with all other documents. The file is updated regularly or whenever new information arise that needs to be added to the Customer's profile or changed existing information.

**8.1.3. Trust accounts**

The Company's employee shall apply the following:

* When the Company establishes a Business Relationship 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 Customer identification procedures prescribed above;
* 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 Customer’s file.

**8.1.4. Electronic gambling/gaming through the internet**

The Company shall apply the following with respect to accounts related to electronic gambling/gaming through the internet:

a) The Company may establish a Business Relationship with Legal Entities, who are licensed by a competent authority of a country of the EEA or a third country, which applies enhanced precautionary measures for the prevention of Money laundering or terrorism financing;

b) The Company shall collect adequate information so as to understand the Customers’ control structure and identification process;

c) In the case that the Customer is a Legal Entity, who offers services (e.g. payment providers, software houses, card acquirers) to the persons mentioned in point (a) above, the Company shall request and obtain, apart from the data and information required by the Manual, adequate information so as to be satisfied that the services are offered pursuant to law. Also, it will obtain information necessary to completely understand the ownership structure and the group in which the Customer belongs, as well as any other information that is deemed necessary so as to establish the Customer’s profile. Additionally, the Company shall obtain the signed agreement between its Customer and Customers' clients;

d) For all the above cases, the decision for the establishment of a Business Relationship is taken by the CEO of the Company. Moreover, the account of the said Client is closely monitored and subject to regular review with a view of deciding whether or not to permit the continuance of its operation. Accordingly, a report shall be prepared and submitted for consideration and approval to the CEO and filed in the Customer’s personal file.

**8.1.5. Customers from countries which inadequately apply FATF’s recommendations**

The FATF 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 Customers from countries, which inadequately apply FATF’s recommendations:

* Exercise additional monitoring process;
* The Company applies, when deemed necessary, enhanced due diligence measures for identifying and monitoring transactions of persons originating from countries with significant shortcomings in their legal and administrative systems for the prevention of Money Laundering and Terrorist Financing.

Based on the said reports, the CO assesses the risk from transactions and Business Relationships with persons from various countries and decides of the countries that inadequately apply the FATF Recommendations. According to the aforesaid decision the Company applies, when deemed necessary, Enhanced Due Diligence Measures for identifying and monitoring transactions of the persons originating from countries with significant shortcomings in their legal and administrative systems for the prevention of Money Laundering and Terrorist Financing.

***8.2. Account Monitoring***

The Company's employees performing an on-going screening of every new deposit regardless of the account verification level. The constant monitoring of the Customer’ accounts and transactions is an imperative element in the effective controlling, as well as to mitigate any potential risk, including the Money Laundering and Terrorist Financing risk. With intent to monitor and collect updated Customer identification data, the Company has implemented a risk based approach. Customers that are classified as higher risk with respect to the Money Laundering and Terrorist Financing risk which the Company faces shall undergo a more complex monitoring as opposed to Customers classified as low/medium risk. The Company’s high risk Customers are categorized of:

* Non face to face Customers with a high monthly turnover;
* PEPs accounts;
* Customers originating from countries, which inadequately apply the Financial Task Force’s recommendations.

Transactions that are not justified by the available information on the Customer, are thoroughly examined so as to determine whether suspicions over Money Laundering or Terrorist Financing arise for the purposes of submitting an internal report.

Customer transactions transmitted for execution, shall be compared and evaluated against the anticipated account’s turnover (total deposits vs. declared profile - to ensure the activity is consistent with the Customer’s profile). Significant deviations are investigated and the findings are recorded in the respective Customer’s file.

The procedures and intensity of monitoring Customer’ accounts and examining transactions on the Customer’s level of risk shall include the following the identification of:

* Transactions that, as of their nature, may be associated with Money Laundering or Terrorist Financing;
* Unusual or Suspicious Transactions that are inconsistent with the Customer's profile.

Where the Account Holder information unambiguously indicates a U.S. place of birth, the Company obtains a record of:

* A self-certification that the Account Holder is neither a U.S. citizen nor a U.S. resident for tax purposes (which may be on an IRS Form W-8 or other similar agreed form);
* A non-U.S. passport or other government-issued identification evidencing the Account Holder’s citizenship or nationality in a country other than the United States; and
* A copy of the Account Holder’s Certificate of Loss of Nationality of the United States or a reasonable explanation of:

a) The reason the Account Holder does not have such a certificate despite relinquishing U.S. citizenship; or

b) The reason the Account Holder did not obtain U.S. citizenship at birth.

PEPs approved by management to open an account will be monitored upon performing a depositing or withdrawal of the funds. The monitoring will include the following:

* Payment method used is consistent with the method mentioned on the PEP's questionnaire;
* Account volume fits the volume mentioned in the questionnaire;
* Negative database screening shows no new results.

The monitoring of accounts and transactions are carried out in relation to specific types of transactions and the Customer's profile, as well as by comparing periodically the actual movement of the account with the expected turnover as declared at the establishment of the Business Relationship. Furthermore, the monitoring covers a dormant accounts exhibiting unexpected movements.

The Company's CEO and CO shall be responsible for maintaining as well as developing of the Customers' on-going monitoring process.

**8.2.1. Customer Identification**

The Company rely on third person (partner) for the implementation of Customer identification.

The Company may rely on third persons only at the outset of establishing a Business Relationship for the purpose of verifying the identity of their Customers. According to the degree of risk any additional data and information for the purpose of updating the Customer’s profile or for the purpose of examining unusual transactions collect and research the company itself.

The partner (in verification process) requests and accepts passports issued by competent authorities of the Customer’s country of origin (passport number, Customer’s name, photo, issuing and expiring date, Country and Customer’s date of birth must appear on the documents obtained). In cases, where the Customer is not a passport holder, then his National Identification Card issued by competent authorities of the Customer’s country of origin or legal residency should be provided (ID/DL number, Customer’s name, photo, issuing and expiring date, Country and Customer’s date of birth must appear on the documents obtained).

In the verification process the partner check whether a Customer is included in the relevant list of persons’ subject to financial sanctions, issued by the United Nations or the European Union based on the United Nations Security Council’s Resolution and Regulation or a Common Position of the European Union’s Council respectively. The Compliance officer is responsible for ensuring that the lists are checked at least once per month.

The Company must be sure that the third person implemented Customer identification system and procedure, which are satisfy of the EU legislation. The Company maintains a separate record for the third person, where it stores the assessment reports of the Customers' identification results and other relevant information (for example identification details, evidence of the data and information).

The Company has access to the data, information and documents obtained as a result of the applying of the procedure establishing identity. The identification data and information obtained for the Customer and Beneficial Owner, are forwarded from the third party to the Company.

Considering the Customer is not present so as to verify the authenticity of his/her signature or that he is the real owner of the account, the Company applies reliable methods, procedures and control mechanisms over the access to the electronic means so as to ensure that it deals with the true owner or the authorised signatory of the account. In the cases, where the transaction instructions are via the internet, the Customer should use his/her login details.

Pursuant to EU legislation, the in addition to Customer identification and due diligence procedures, the Company shall:

* Ensure that the Customer identification records remain completely updated with all relevant identification data and information throughout the Business Relationship;
* Check, on a regular basis, the validity and adequacy of the Customer identification data and information it store, especially for high risk Customers;
* The Company takes all necessary action, by applying the Customer identification and due diligence procedures, to collect the missing data and information, the soonest possible, so as to identify the Customer (if necessary).

 Profile's information shall be reviewed and updated at a minimum on an annual basis or at any point in time where relevant data is missing from the Customers’ file. Valid proof of identity shall be requested upon the elapse of the document validity or at any point in time where relevant data is missing from the Customer’s file. Valid proof of residence – updated records and/or documentation shall be requested on a yearly basis or at any point in time where relevant data is missing from the Customer’s file. The Company is always reserving its right to request for further documentation and/or clarifications according to each case.

**8.2.2. Proof of Residence (Natural Person)**

The Company accepts recent, up to 3 (three) months old, documents (stating the Customer’s first and last name and residential address):

* Utility bill (telephone, electricity, water, gas, internet, phone bills, cable TV, municipality bills, common expenses bills etc.);
* Local authority tax bill;
* A bank statement or any other document same with the aforesaid.

The Company does not accept receipts, insurance contracts, cut/destroyed documents, documents not in the name of the Customer and documents in the name of Legal Entities (even if the document includes the name of the Customer).

Utility bills including only P.O. Boxes are not accepted.

If utility bills are not in the name of the Customer, the following alternative must be completed instead:

* Any written declaration from the police or Court stating the Customer’s address;
* Valid tenancy agreement and a signed, notarised/certified, written statement from the party from whom the Customer rents a property. This letter must be signed from the third party and not the Customer himself;
* The Company’s CO shall exercise his discretion as to what other documents, where the above cannot be obtained, may be acceptable.

Where a new residential address cannot be proved, because the address is only temporary or verification evidence is not yet available, then the previous address should be verified. The current address should be verified as soon as practically possible afterwards. Notes should be held on file to clarify the situation.

**8.2.3. Information of the Payment methods**

* Bank Transfer (provided information of bank details, from which will be income deposits to the Customer's account - bank name and address, account number, IBAN, SWIFT/BIC code);
* Card verification (the Customer must cover the middle digits and leaving exposed the first six (6), the last four (4), the expiry date and the card holder’s name).

During the Business Relationship this information will be applying for ensuring that the payment method belongs to the Customer, and his/her details are correct and match to the early requested information.

**8.2.4. Negative Database Screening**

This is performed by the Company using, an aggregator of negative databases:

* Sanction list of EU, EU relating to Al-Qaida & Taliban targeted countries in relations to Money Laundering and Terrorism Financing;
* European Union terrorism list – the EU publishes a list of known terrorists that businesses are not to provide services and transactions for. The list also contains frozen assets which require immediate reporting to the EU police forces once used in the system;
* FBI most wanted;
* Interpol most wanted;
* FATF SDC, SDN and blocked entities list;
* UN consolidated list;
* World bank debarred parties.

With regard to the issue of corruption, one useful source of information is the Transparency International Corruption Perceptions Index which can be found on the website of Transparency International at [www.transparency.org](http://www.transparency.org/).

With regard to the issue of adequacy of application of the FATF Recommendations, the Company shall retrieve information from the country assessment reports prepared by the FATF or other regional bodies operating in accordance with FATF’s principle.

**8.2.5. Additional Approvals by CEO**

* A corporate account opening;
* A deposit rejecting;
* Funds withdrawals;
* Acceptance for establishing and during a Business Relationship with PEP.

**8.2.6. Deposits, Withdrawals**

The Company does not allow Customers to use third party funds. All deposits the Customers must to send only from himself/herself owned accounts and payment cards.

Funds withdrawal can be possible only to the Customer owned bank account. Exceptional requests for withdrawal in another source due to legit reason than the one used for depositing may be considered upon submitting supporting documentation and after of the Company’s CEO acceptance (e.g. the bank account no longer exists, death of the Customer). Please see deposit & withdrawal procedure in Appendix 7.

**9. Recognition and Reporting of Suspicious Transactions / Activities to the FIU**

The Company's employees are obliged to reporting Suspicious Transactions for further investigation by using the form. The CO receives information and internal suspicious reports, which are considered to be knowledge or suspicion of Money Laundering and Terrorist Financing activities and upon their review decides whether he/she has a solid evidence to notify the FNTT by completing the evaluation form.

The CO must inform the FNTT of each operation equal to or exceeding EUR 15000, whether it was a single operation or several related operations. The information must be provided to the FNTT no later than 3 days after the operation.

***9.1. Suspicious Transactions***

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 Customer's known, legitimate business or personal activities or with the normal business of the specific account, or in general with the profile that the Company has created for the Customer.”

The Company shall ensure that it maintains adequate information and knows enough about its Customers' activities in order to recognize on time that a transaction or a series of transactions is unusual or suspicious.

Examples, in accordance with the EU legislation, of what might constitute Suspicious Transactions/activities related to Money Laundering and Terrorist Financing are listed in Appendix 8 of the Manual. The relevant list however, includes examples that do not apply directly to the Company’s business model such us examples that relate to cash transactions.

Moreover, the relevant list is not exhaustive nor it includes all types of transactions that may be used, nevertheless it can assist the Company and its employees (especially the MLRO) in recognizing the main methods used for Money Laundering and Terrorist Financing. The detection by the Company of any of the transactions contained in the said list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds, the nature and economic/business purpose of the underlying transaction, and the circumstances surrounding the particular activity.

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 which is mentioned in Appendix 8 of this Manual;
* Investigate Suspicious Transactions, which creates the belief or suspicion of money laundering;
* The CO should to explain each decision of disclosing or not this information to the FIU.

The employees of the Company will receive continuous training, educating them about the means of identifying Suspicious Transactions. All employees must be clearly instructed and trained not to inform or “tip-off” the suspected party of a pending investigation.

The Company is responsible for ensuring prompt allocation of the resources for a complete investigation of the incident and a timeframe for the corrective measures.

***9.2. Submission of information to the FIU***

The Company shall ensure that in the case of a Suspicious Transaction investigation by the FIU the Company will be able to provide without delay the following information:

* The identity of the account holders;
* The identity of the Beneficial Owners of the account;
* The identity of the persons authorised to manage the account;
* Data of the volume of funds or level of transactions flowing through the account;
* In relation to specific transactions:

a) The origin of the funds;

b) The type and amount of the currency involved in the transaction;

c) The form in which the funds were placed;

d) The type and identifying number of any account involved in the transaction.

The Company may subsequently wish to terminate its relationship with the Client concerned for risk avoidance reasons. In such an event, the Company exercises particular caution not to alert the Customer concerned that a suspicious report has been submitted to the FIU.

After submitting the suspicious report the Company adheres to any instructions given by the FIU and, in particular, as to whether or not to continue or suspend a particular transaction or to maintain the particular account active.

**10. Record-Keeping Procedures**

The Customers' files shall be a set of the documents and information executed in accordance with this Manual and containing identification data of the Customers, evidences of legal capacity and competences of the Customers and their representatives, and others documents that proof legal side of establishing a Business Relationships.

***10.1. The Company shall maintain records of:***

* The Customer identification documents and information obtained during the Customer identification and due diligence procedures, as applicable;
* Relevant evident material and details of all Business Relations and transactions;
* The details of all relevant records with respect to the provision services to Customer;
* Relevant documents of correspondence with the Customers, with whom they keep a business relation;
* Details of actions taken in respect of internal and external suspicion reports;

The documents/data of mentioned above shall be kept for a period of at least five (5) years, which is calculated after the execution of the transactions or the termination of the Business Relationship.

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

The Company keeps all documents in electronic form (in cases of additional investigations requests, reports and other documents can be stored in paper copy), provided that it shall be able to retrieve the relevant documents/data without undue delay and present them at any time to FIU after a relevant request.

The internal auditor shall review the adherence of the Company to the above, at least annually.

***10.2. Certification and language of documents***

* Documents data is obtained in electronic copies. In case of suspicion, documents are requested to be notarized;
* A true translation (notarized and legalized) shall be attached in the case that the documents of point above are in a language other than English.

**11. Employees’ Obligations, education and training**

Obligations:

* The Company’s employees shall be personally liable for failure to report information or suspicion, regarding Money Laundering or Terrorist Financing;
* The employees must cooperate and report, without delay anything that comes to their attention in relation to transactions or any activity in a Customers' accounts, for which there is a slight suspicion that are related to Money Laundering or Terrorist Financing.

Education and Training:

The Company shall ensure by introducing a complete employee’s education and training program that all employees are fully aware of their legal obligations according to inter alia:

* The systems and procedures in accordance to this Manual;
* Directive (EU) 2018/843 on the prevention of the use of the financial system for the purposes of Money Laundering or Terrorist Financing;
* Prevention and Suppression of Law on the prevention of money laundering and terrorist financing, 19 June 1997 No. VIII-275, of Lithuanian Republic;

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 Lithuania and EU.

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. On-going training shall be given at regular intervals so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments.

The CEO 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 Company's employees.

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

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

Appendix 1

INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

INFORMER’S DETAILS

Name: …………………………………………………………………………………….

Tel: ………………………………………………………………………………………...

Position: ………………………………………………………………………………...

Reference number: ………………………………………………………………..

This report is (to circle necessary):

\* A request for consent for a transaction, which is not yet completed

\* A report on a transaction, which has taken place, and I consider it as suspicious

\* Report on other business related activity, which I consider suspicious

CUSTOMER’S DETAILS

ID Number: ................................

Name: ................................................................................................................................................

Tel: .............................................................................................

INFORMATION/SUSPICION

Date of transaction: ………………………………………………………………..

Amount: ………………………………………………………………………………….

A transaction number: …………………………………………………………….

Reason(s) for suspicion:

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

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

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

........................................................................................................................................................…

.......................................................................................................................................................….

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

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

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

Informer’s Signature .........................................… Date .......................................……..

Appendix 2

INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

Reference number: ...................................…

Customer’s ID: .....................…………………….

Amount: ………………………………………….

Informer: ...............................................………….

Position: ………………………………………….

INQUIRIES UNDERTAKEN (Brief Description)

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

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

........................................................................................................................................................…

ATTACHED DOCUMENTS

.......................................................................................................................................................…..

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

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

CO’S DECISION

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

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

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

FILE NUMBER: ..............................................

CO’S NAME, SIGNATURE……………………………………………………………………..

DATE ....................................................

Appendix 3

MLRO REPORT TO THE FNTT

*1. GENERAL INFORMATION*

Company’s Name……………………………………………………………………………………

Address, where Client’s account is kept…………………………………………………………….

Date, when a Business Relationship established..…………………………………………………..

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

*TRANSACTION(S)*

Natural Person

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name (s) of the Account’s Beneficial Owner (s) | Name (s) of the Account’s Authorised signatory (ies) | Date and place of birth | Nationality and passport number | Residential address(es) | Business address(es) | Occupation |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Legal Entity

Legal Entity’s name, country and date of incorporation

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

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

........................................................................................................................................................…

Business address

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

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

........................................................................................................................................................…

Main activities

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

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

........................................................................................................................................................…

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Name | Nationality and passport number | Date of birth | Residential address | Occupation |
| Registered shareholder (s) |  |  |  |  |  |
| Beneficial Owner (s) (if differs from above) |  |  |  |  |  |
| Directors |  |  |  |  |  |
| Account’s Authorised signatory (ies) |  |  |  |  |  |

*3. DETAILS OF SUSPICIOUS ACTIVITIES*

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

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

........................................................................................................................................................…

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

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

........................................................................................................................................................…

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

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

........................................................................................................................................................…

........................................................................................................................................................…

The above report should be accompanied by photocopies of the following:

1. For natural persons: The relevant pages of the Client’s passport or ID card evidencing identity.

2. For legal entities: Certificates of incorporation, directors and shareholders.

3. All documents relating to the Suspicious Transaction(s).

Name, Signature ...........................................................................................................................…

Date …………………………………..

Appendix 4

CUSTOMER ACCEPTANCE POLICY

Money Laundering is the participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities including fraud, corruption, organized crime, terrorism, and many other crimes. Predicate offences for money laundering are defined by local law in the diverse jurisdictions.

Generally, the money laundering process consists of three stages:

Placement

Introduction of cash or other physical valuables originating from illegal / criminal activities into financial or non-financial institutions.

Layering

Separating the proceeds of criminal activity from their source through the use of layers of complex financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.

Integration

Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds.

 Financial/non-financial institutions may be misused at any point in the money laundering process.

CUSTOMER ACCEPTANCE POLICY ON A RISK BASED APPROACH

 The Company’s Customers Acceptance Policy on a risk based approach is prepared by the compliance officer after detailed assessment of the risks faced by the Company. In this regard the Company applies appropriate measures and procedures, on a risk based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be higher.

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

* When establishing a business relationship;
* When carrying out transactions amounting to EURO 15,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
* 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 customer identification data.

As a minimum requirement, the following criteria have to be met for accepting new clients:

* Identification and verification of the customer (e.g. Proof of identification);
* Identification and verification of the beneficial owner(s)

Further details on the documents required to open an account can be found on the Company’s KYC procedure.

CRITERIA FOR NOT ACCEPTING CUSTOMERS

Categories of customers who are not acceptable for establishing a business relationship or an execution of an occasional transaction with our Company are the following:

* Customers, 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;
* Potential Customers that require to open anonymous account;
* Potential new Customers that do not appear to be legitimate are declined;
* Shell Banks.

Further details on not acceptable clients can be found on the Company’s AML Manual.

Additionally, the Company does not accept Customers, who are residents of:

Afghanistan

Algeria

Bangladesh

Bolivia

Cambodia

Central African Republic

Cuba

Democratic People's Republic of Korea (DPRK)

Democratic Republic of the Congo

Ecuador

Egypt

Ghana

Iraq

Iran

Island

Japan

Lebanon

Libya

Macedonia

Mali

Morocco

Myanmar

Namibia

Nepal

Palestine

Pakistan

Qatar

Saudi Arabia

Somalia

South Sudan

Sudan

Syria

USA

Venezuela

Yemen

Zambia

Zimbabwe

This list can be changed according to the company's internal policy and changes by EU laws.

Additionally, the Company runs a risk assessment test for each of its Customer in order to identify, which Customer have a high ranking on money laundering or terrorist financing.

Based on the extent and the combination of the risk criteria the Company will identify the ranking of each Customer in relation to the risk faced by the Company on Money Laundering or Terrorist Financing.

Appendix 5

DORMANT ACCOUNT POLICY

The Dormant Account Policy lays down the procedure to be followed regarding the Dormant Customers accounts and the procedure to be followed, when receiving an instruction for an account, which is classified as Dormant. This policy gives full description of the time period and method considered for classifying an account Dormant and also various steps required to be adhered for re-activating such Dormant accounts.

Definition

An account shall be classified to be Dormant if it is inactive or remains non-operational by its holder for a specified period of time. The dormancy period for all customer accounts will stand at 1 (one) year. For instance, if no transactions have been carried out in relation to the account by or on the instructions of the account holder for a minimum period of 1 (one) year, it will be classified as a Dormant account.

Application

The Company's employees shall review accounts, at least annually, to determine status as "Dormant". The Dormant accounts will be frozen and the Customer will not be permitted to undertake any further transaction in such account. The Company’s employee sends a request to the Customer about reason of an inactivity and request to Customer to close the account, if it no longer required.

1) In case of Customer’s consent to close the account, the Company informs in writing (via its registered email) the Customer about the termination of his/her account.

2) In case the Customer wishes to keep his/her account then KYC/CDD procedures as describes in Company’s AML Manual are applied.

3) If the Company can not establish contact with the Customer the account classified as “Dormant Whereabouts Unknown” (DWAU)”. In these cases the Company consults with a lawyer of how to treat these accounts. In case of possible request from an owner of a DWAU account for a transaction, the Company's employee will apply KYC/CDD procedure as described in AML Manual and reactivate the account.

Monitoring

The Company will review and monitor the effectiveness of this Dormant Account Policy and arrangements to identify and, where appropriate, correct any deficiencies. It will assess, at least on a yearly basis the efficiency of the procedures set in this Policy.

Appendix 6

POLITICALLY EXPOSED PERSON (PEP) ACCEPTANCE FORM

1. CUSTOMER INFORMATION

Full name……………………………………………………………………………………………..

Passport/ID number………………………………………………………………………………….

I am a PEP, due to the fact that:

\* I am the (described position)...…………………………………………………………………….

\* I am a family member of (describe full name, title)………………………………………………..

Our relationship is (spouse or a person considered to be equivalent to a spouse, a child and their spouse or a person considered to be equivalent to a spouse, parent):................................................................................…

\* I am a person, which is close associates with PEP........................................................................…

2. SOURCE OF FUNDS

\* What is your intended purpose for the Business Relationship with us?........................................…

\* What is your planned monthly turnover of our platform?

........................................................................................................................................................…

\* Please provide the details of the payment methods you intend to use for the account deposit?

\*\* Bank details ............................................................................................................................…...

........................................................................................................................................................…

........................................................................................................................................................…

\*\* Card verification

Selfie, where can see a Customer’s name on the front of the card and expiry date. Additionally, show first six and last four digits only; the other numbers have to be hidden by the customer, before he send to us the card’s copy.

\* What is the source of funds that you plan to deposit (mark the relevant option):

- self -employment incomes

- insurance claim payments

- trust/inheritance

- proceeds from a legal case or action

- employment incomes

- retirement/pension incomes

- investment incomes/savings

- loan

- tax return

- property tenancy

- other (please explain)

3. CONTACT DETAILS

\* Full address (house, ap. number, street, city, country, post code):

........................................................................................................................................................…

\* Telephone number, email address:

........................................................................................................................................................…

4. REQUIRED DOCUMENTS

\* passport

\* proof of residence (utility bill, bank statement etc. not older than 3 months)

\* proof of funds (not older than 3 months)

\* recommendation letter from trusted institution (bank, notary, lawyer; dated, signed and stamped)

5. CUSTOMER CONFIRMATION

I hereby confirm that all information disclosed above is complete, true, accurate and I agree to promptly notify you of any changes in this information or it ceases to be true and accurate.

Customer’s name, signature...........….………………………………………………………………………

Date.........................................…..

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CEO APPROVAL

Customer ID……………………………………………………………………………………...

Date of account opening……...…………………………………………………………………..

CEO’s name, signature…….……………………………………………………………………..

Date ....................................................

Appendix 7

DEPOSIT & WITHDRAWAL PROCEDURE

The purpose of this Policy is to lay down the Company’s internal practice, measures, procedures and controls with regards to the treatment of Deposits & Withdrawals.

1. Deposit & Withdrawals via Bank Wire:

A) DEPOSIT

The Company’s employees receives and checks the Deposit Report provided by the relevant payment services providers, with which the Company holds segregated client accounts.

If upon review, the employee has identified the Customer name, he/she enrolls funds to the Customer's account. If upon the review, the employee identifies any deposits with lack of details, he/she investigates this cases and requests information to payment service provider and, additionally, corroborant documents from the Customer.

The Company does not accept and prohibits third party or anonymous deposits.

B) WITHDRAWAL

Initial Deposit + Profits (General Policy):

The Company as part of its monitoring controls and measures will proceed as follows in the case of a withdrawal request:

* The Company will at all times refund the amount(s) initially deposited back to the same source (i.e. same remitter). If the Customer uses more than one bank account, the Company will refund funds to each bank account, from where its have been deposited;
* Profits can be sent in any of the bank accounts used;
* Third party withdrawals or withdrawals to an anonymous accounts are prohibited;
* The employee checks the amount for withdrawal with the available amount in the Customer's account;
* If the Company cannot proceed with the withdrawal per the Swift provided by the Customer, the Company's employee requests from Customer a bank account statement in order to confirm Customer’s bank account details;
* The Customer can receive his/her profits in a different bank account (i.e. bank wire) other than the one used for an initial deposit, if the Customer will provide sufficient proof that the new bank account belongs to him/her (to account's owner).

2. Deposit & Withdrawals via Payment Cards:

A) DEPOSIT

The Company’s employees receives and checks the Deposit Report provided by the relevant payment services providers, with which the Company holds segregated client accounts. The Customers should deposit their account only by them owned payment cards.

If the Company's employees cannot verify the owner of the payment card because of its “anonymous”, the Customer must provide further documentation and information for proof of the card's ownership. If the Customer fails to provide, then funds are refunded back to the same source.

When the Company requests to verify the Customer's payment card, it is must be done in clean copy. If the payment card being expired, the Customer must provide new valid payment card. If he/she fails to provide, then funds are refunded back to the same source.

If upon review the Company's employee cannot verify the owner because it belongs to a third party, then funds are refunded back to the same source.

B) WITHDRAWAL

* Company will at all times refund the amount(s) initially deposited back to the same source (i.e. to the account that funds were initially deposited). If the Customer uses more than one payment card, the Company will refund funds to each payment card, from where its have been deposited;
* Third party refunds or refunds to an anonymous accounts are prohibited;
* All funds withdrawals after deal are possible only to the Customer bank account.

Appendix 8

EXAMPLES OF SUSPICIOUS TRANSACTIONS/ACTIVITIES RELATED TO MONEY LAUNDERING AND

TERRORIST FINANCING

1. Money Laundering:

\* Transactions with no discernible purpose or are unnecessarily complex;

\* Use of foreign accounts of companies or group of companies with complicated ownership structure, which is not justified based on the needs and economic profile of the Customer;

\* The size of the transactions requested by the Customer do not comply with his/her usual practice and business activity;

\* Large volume of transactions and/or money deposited or credited into, an account when the nature of the Customer’s business activities would not appear to justify such activity;

\* The Business Relationship involves only one transaction or it has a short duration;

\* Any transaction the nature, size or frequency appear to be unusual, e.g. cancellation of an order, particularly after the deposit of the consideration;

\* Transactions, which are not in line with the conditions prevailing in the market, in relation, particularly, with the size of the order and the frequency;

\* Settlement of the transaction by a third person which is different than the Customer, which gave the order;

\* Transfer of funds to and from countries or geographical areas which do not apply or they apply inadequately FATF’s recommendations on Money Laundering and Terrorist Financing;

\* A Customer provides unusual or suspicious identification documents that cannot be readily verified;

\* A Customer that makes frequent or large transactions and has no record of past or present employment experience;

\* Difficulties or delays on the submission of the financial statements or other identification documents, of a Customer/Legal Entity;

\* The stated occupation of the Customer is not commensurate with the level or size of the executed transactions;

\* Financial transactions from non-profit or charitable organizations for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction;

\* Unexplained inconsistencies arising during the process of identifying and verifying the Customer (e.g. previous or current country of residence, country of issue of the passport countries visited according to the passport, documents furnished to confirm name, address and date of birth etc.);

\* Complex trust or nominee network;

\* Transactions or company structures established or working with an unneeded commercial way, e.g. companies with bearer shares or bearer financial instruments or use of a postal box.

2. Terrorist Financing

*Sources and methods*

The funding of terrorist organizations is made from both legal and illegal revenue generating activities. Criminal activities generating such proceeds include kidnappings (requiring ransom), extortion (demanding “protection” money), smuggling, thefts, robbery and narcotics trafficking. Legal fund raising methods used by terrorist groups include:

\* Collection of membership dues and/or subscriptions;

\* Sale of books and other publications;

\* Cultural and social events;

\* Donations;

\* Community solicitations and fund raising appeals.

Funds obtained from illegal sources are laundered by terrorist groups by the same methods used by criminal groups. These include cash smuggling by couriers or bulk cash shipments, structured deposits to or withdrawals from bank accounts, purchases of financial instruments, wire transfers by using “straw men”, false identities, front and shell companies as well as nominees from among their close family members, friends and associates.

*Non-profit organizations*

Non–profit and charitable organizations are also used by terrorist groups as a means of raising funds and/or serving as cover for transferring funds in support of terrorist acts. The potential misuse of non-profit and charitable organizations can be made in the following ways:

\* Establishing a non-profit organization with a specific charitable purpose but which actually exists only to channel funds to a terrorist organization;

\* A non-profit organization with a legitimate humanitarian or charitable purpose is infiltrated by terrorists who divert funds collected for an ostensibly legitimate charitable purpose for the support of a terrorist group;

\* The non-profit organization serves as an intermediary or cover for the movement of funds on an international basis;

\* The non-profit organization provides administrative support to the terrorist movement.

Unusual characteristics of non-profit organizations indicating that they may be used for an unlawful purpose are the following:

\* Inconsistencies between the apparent sources and amount of funds raised or moved;

\* A mismatch between the type and size of financial transactions and the stated purpose and activity of the non-profit organization;

\* A sudden increase in the frequency and amounts of financial transactions for the account of a non-profit organization;

\* Large and unexplained cash transactions by non-profit organizations;

\* The absence of contributions from donors located within the country of origin of the non-profit organization.