ANTI-MONEY LAUNDERING AND COUNTER TERRORIST FINANCING COMPLIANCE POLICY

Nemuneris UAB

Contents

I. GENERAL PROVISIONS

1. Nemuneris UAB (hereinafter – the Company) is a virtual currency exchange and virtual currency wallet company performing ICO, acting according to the laws of the Republic of Lithuania. The Company is committed to conduct business operations in a transparent and open manner consistent with its regulatory obligations.

2. This policy implements the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania, dated 19 June 1997 No VIII-275 No XIII-2584 (hereinafter – the Law).

3. The Company by implementing measures to prevent money laundering and / or terrorist financing is guided by the following main documents issued by the Director of the Financial Crime Investigation Service:

- Technical Requirements for the Customer Identification Process for Remote Identification Authentication via Electronic Devices for Direct Video Transmission approved by the Director of the Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania on November 30th 2016 by Resolution No. V-314 "For the Technical Requirements for the Customer Identification Process for Remote Identification Authentication via Electronic Devices for Direct Video Transmission" (hereinafter – Technical Requirements).
- Resolution No. V-240 of December 5th of 2014 of the Director of Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania "On the Approval of the List of Criteria for Money Laundering and Suspicious or Unusual Monetary Operations or Transactions Identification".
- Resolution No. V- of 5 January 10th of 2020 of the Director of Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania "On the Approval of Guidelines for the Depositary virtual currency wallet operators and virtual currency exchange operators to prevent money laundering and/ or terrorist financing."
- Resolution No. V-273 of October 20th of 2016 of the Director of Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania "On the Approval of Guidelines for the Supervision of Financial Crimes for the Implementation of International Financial Sanctions in the Field of Regulations of the Ministry of Internal Affairs of the Republic of Lithuania."

4. The supervisory authorities have the right to initiate inspections of implementation of the money laundering and/or terrorist financing prevention measures set out in the Law at their own initiative on the basis of the supervisory authorities' inspection plan (supervision plan).

5. The supervisory authorities may also initiate inspections relating to possible breaches of the Law upon receiving a report or any other data in which the circumstances of the possible breaches of the Law are recorded.

6. The following shall be considered as a serious breach of the Law:

- failure to comply with the customer due diligence requirements,
- failure to comply with the requirements for reporting of suspicious monetary, virtual currency exchange operations or transactions in virtual currency,
- failure to comply with the requirements for the storage of information,
- where an obliged entity has not put in place the internal control procedures.

7. Information on the beneficial owners of the Depository Virtual Currency Wallet Operator and Virtual Currency Exchange Operator must be submitted to the Legal Entities Participant Information System (JADIS) Manager.

8. The Company will not carry out activities or provide services in another country to such an extent that only non-essential functions or services would remain in the Republic of Lithuania and they would be performed or provided exclusively to customers of another country, or the Company would essentially no longer carry out activities in the Republic of Lithuania.

II. DEFINITIONS

9. **"Money laundering"** or "ML" the following conduct, when committed intentionally, shall be regarded as money laundering:

a) The conversion or transfer of property, knowing that such property is derived from Criminal Activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action.

b) The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from Criminal Activity or from an act of participation in such an activity.

c) The acquisition, possession, or use of property, knowing, at the time of receipt, that such property was derived from Criminal Activity or from an act of participation in such an activity.

d) Participation in, association to commit, attempts to commit and aiding, abetting, facilitating, and counselling the commission of any of the actions referred to in points (a), (b) and (c).

Money Laundering shall be regarded as such regardless of where the activities that generated the property to be laundered are carried out.

10. **"Terrorist financing"** or "TF" shall mean any act that under the UN International Convention for the Suppression of the Financing of Terrorism adopted on 9 December 1999 is treated as an offense including, but not limited to any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

11. **"Suspicious activity or transaction"** shall mean a monetary operation or transaction relating to property which is suspected of being derived, directly or indirectly, from a criminal activity or from involvement in such an act and/or is, suspected to be associated with terrorist financing.

12. **"Politically Exposed Person" ("PEP")** shall mean natural persons who are or have been entrusted with Prominent Public Functions and Close Family Members or Close Associates of such persons as defined in the AML Law.

13. **"Risk-Based Approach"** or "RBA" shall encompass identifying, assessing, and understanding the ML/TF risks to which the Company is exposed and to take measures proportionate to those risks for the purpose of mitigating them effectively. This means that the range, degree, frequency, or intensity of controls will be more comprehensive in situations assessed as posing a higher ML/TF risk while these measures will be reduced in situations assessed as posing a lower ML/TF risk. Applying a RBA, thereby, allows the Company to target its resources in the most efficient manner. Situations assessed as posing a lower risk must never imply that control measures are not applied.

14. **"Business relationship"** shall mean a business, professional or commercial relationship between the Company and the customer, which arises out of the business of the Company, and is expected by the Company, at the time when contact is established, to have an element of duration.

15. **"Occasional transaction"** shall mean a transaction that is not carried out as part of a business relationship.

16. **"Customer"** shall mean natural person or legal entity performing monetary operations or transactions with the Company and using The Company's products or services.

17. **"Person"**, unless specified explicitly, shall mean any natural person and/or legal entity.

18. **"Criminal Activity"** shall mean any criminal activity as defined by the Criminal Code of the Republic of Lithuania and will as a minimum encompass following offenses as defined by the most recent EU Anti-Money Laundering Directive.

19. **"Regulatory Requirements"**, unless specifically stated, shall mean any law, statute, regulation, order, judgement, decision, recommendation, rule, policy, or guideline passed or issued by parliament, government, or any competent court.

20. **"Target Territory"** shall mean a foreign country or area with very little, or no tax included in the List of Target Territories established by the Minister of Finance of the Republic of Lithuania and where persons register with the aim of achieving minimum or no tax obligations.

21. **"Virtual Currency"** shall mean an instrument with a digital value, but without the legal status of currency or money, which is not issued or underwritten by a central bank or other public authority, and which is not necessarily linked to a currency, but which is recognized by natural or legal persons as an exchange instrument and which can be transferred, kept and traded by electronic means.

22. **"Virtual Currency Exchange Operator"** shall mean legal entity established in the Republic of Lithuania, or a branch of a legal entity of a Member State of the European Union or of a foreign state established in the Republic of Lithuania, offering the services of exchange, purchase and/or sale of virtual currencies for remuneration.

23. **"Virtual Currency Wallet Operator"** shall mean a legal person who is established in the Republic of Lithuania or a branch, established in the Republic of Lithuania, of a legal person of a Member State of the European Union or a foreign state and who provides services of management of custodian virtual currency wallets on behalf of the customers.

24. **"Virtual Currency Wallet"** shall mean virtual currency addresses generated with the public key for storing and managing virtual currencies entrusted to other natural or legal persons (third parties) but remaining their property.

25. Other definitions used in this Policy are those defined in the Law.

III. INTERNAL AML CONTROLS

26. The Company must set out AML/CFT internal controls and relevant policies, procedures covering:

- **a.** Roles and responsibilities over ML/TF prevention, including access to all information needed to perform daily duties according to roles and applicable laws, Internal reporting
- **b.** Business-wide ML/TF risk assessment and customer risk scoring
- **c.** Identification and verification of customer and beneficial owner,
- **d.** Sanctions and Politically Exposed People (PEP) screening,
- **e.** Ongoing due diligence,
- **f.** Transaction monitoring and Suspicious activity reports (SAR) to the Financial Crime Investigation Service (FCIS),
- **g.** Constant employee training,
- **h.** Record keeping requirements.

27. Internal controls in place and related procedures must be updated when:

- European Commission completes supranational ML/TF risk assessment (announced at http,//ec.europa.eu),
- Lithuania completes national ML/TF risk assessment,
- The FCIS orders to tighten internal control procedures,
- There are significant changes in management structure and business nature,
- Gaps are identified during the periodical quality assurance process.

28. An annual audit will be performed to assess the internal controls and their compliance with legal AML/CTF requirements.

IV. ROLES AND RESPONSIBILITIES, INTERNAL REPORTING

29. **The Board** has a critical oversight role – as the senior-most management of the company, they should approve and oversee policies for risk, risk management and compliance. The Board also should have a clear understanding of the ML risks, including timely, complete, and accurate information related to the risk assessment to make informed decisions. Along with the General manager, the Board should appoint a qualified Head of AML (MLRO) with overall responsibility for the AML function and provide this senior-level officer with sufficient authority that when issues are raised, they get the appropriate attention from the Board, the General manager and the business lines. Before appointing General manager and Head of AML (MLRO), the Board is responsible for assessing their work experience, education and qualifications to perform their respective duties and manage ML/TF risks. The Board is responsible for the overall AML/CTF compliance policy of the Company and ensuring adequate resources are provided for the proper training of staff and the implementing of risk systems. The Board will receive and consider quarterly compliance reports presented by the Head of AML (MLRO). The Board is responsible for ensuring that the Head of AML (MLRO) is a Lithuanian resident. The Company ensures that one of the Board members are appointed to be responsible for the implementation of AML/CTF measures in the Company. The Company is responsible for ensuring that the Head of AML (MLRO) and Board member responsible for AML/CTF do not represent other companies dealing with virtual currencies.

30. **Board member responsible for AML/CTF** must possess sufficient knowledge, skills, and experience, commit sufficient time to perform his/her functions which primarily involve overseeing, monitoring, and reporting on the emerging risks, to guarantee that the Company business processes and transactions follow all relevant legal and internal guidelines and make AML/CTF compliance a top priority:

- Promotes a culture of compliance and sends a strong message that AML compliance is a Company-wide responsibility.

- Implements appropriate and effective organizational and operational structure necessary to comply with the AML/CTF strategy, paying particular attention to the

sufficient authority and the appropriateness of the human and technical resources allocated to the AML/CTF function.

- Ensures that the AML/CTF policies, procedures and internal control measures are adequate and proportionate, considering the characteristics of the Company and the ML/TF risks to which it is exposed.

- Initiates discussions on significant AML/CTF concerns with the Board, as well as the need for additional resources.

- Provides sound and practical advice on compliance with regulatory requirements and general compliance matters.

- Assures that periodical reporting to the Board is provided with sufficiently comprehensive and timely information and data on ML/TF risks and AML/CTF, international sanctions compliance.

- Ensures that reporting covers Company's engagements and communications with the FCIS, without prejudice to the confidentiality of SARs, and any ML/TF-related findings of the competent authority against the Company including measures or sanctions imposed.

31. **The Head of AML (MLRO)** is responsible for managing compliance risks, reviewing company's policies and procedures, and monitoring compliance issues. The Head of AML (MLRO) is responsible for preparing monthly and quarterly reports for consideration to the Board regarding AML/CTF function. The Head of AML (MLRO):

- Is key person to communicate with and timely report to relevant regulating authorities (Financial Crime Investigation Service (FCIS), Bank of Lithuania (BoL)).

- Participates in AML/CTF/International sanctions internal and external audits.

- Acts as the first point of escalation for all AML/CTF/International sanctions issues from staff.

- Develops, maintains, and updates risk-based approach to AML/CTF and international sanctions.

- Revises and updates AML/CTF/International sanctions policies and procedures at least once per year or if there are changes in internal processes, regulatory requirements, or standards.

- Reports to the Management Board regarding suspicious operations and effectiveness of AML/CTF, International sanctions controls and procedures whenever appropriate but not less than once per quarter.

- Identifies situations of higher ML/TF risk and advises employees on the application of additional measures, including enhanced ongoing monitoring and other controls imposed on high-risk customers.

- Understands the functioning and design of the transaction monitoring system, keeps a record of all internal investigations carried out and ensures that the Company's internal controls comply with guidance provided by the FCIS.

- Oversees efficient transaction monitoring implementation and regularly updates the list of examples of unusual activity.

- Performs internal investigations on international sanctions, is responsible for the freezing of customers' accounts and funds, and other actions as required by the relevant sanctions' programs.

- Keeps up to date with ongoing legislation changes, regulatory recommendations, and industry best practices on AML/CTF and international sanctions compliance.

- Duly informs all staff about the ML/TF/International sanctions risks, including ML/TF/International sanctions methods, trends, and typologies.

- Organizes the AML/CTF, International sanctions training course, assesses the need of additional and specialized trainings. Is responsible to draft and update yearly training plan and ensures ongoing employee education in AML/CTF and International sanctions area.

- Maintains required AML related logs and information within the Company

32. **Compliance Officer (CO)** is responsible for compliance with all legal requirements and internal procedures, forms and supervise Company's internal control and compliance program:

- Develops framework for business-wide and customer ML/TF risk assessments in line with legal requirements and best practice and proposes to the Management Board the measures to be taken to mitigate identified risks.

- Conducts regular testing of Company's functions to identify areas of non-compliance within established policies, controls and procedures, and initiates solutions to address identified risks.

- Conducts oversight and ensures that adequate AML/CTF/International sanctions related policies and procedures are put in place, kept up to date (reviewed in response to regulatory changes and updated at least once a year), and implemented effectively on an ongoing basis.

- Is key person to consult the Management Board, the Head of AML (MLRO) and other relevant staff regarding compliance related issues, including advice to senior management on high-risk customers from compliance perspective.

- Reports on Company's activity, the ML/TF risk assessment, on resources, on policies and procedures on at least an annual basis to the Management Board.

- Participates in introducing new products to ensure proper compliance with the AML/CTF and international sanctions requirements.

- Oversees the preparation and implementation of an ongoing AML/CTF/International sanctions training program.

33. **Other staff members** are responsible to familiarize them with this Policy, other internal procedures related to their job role and understanding responsibilities and ensure that AML/CTF procedures are adhered to. Other staff must report all suspicious activity to the Head of AML (MLRO).

34. The Company shall notify the Financial Crimes Investigation Service in writing (e-mail: documentas@fntt.lt) about the appointment of employees described in points 30 and 31 of this Policy, providing the data and contact information of the appointed employees (e-mail address, phone number).

V. BUSINESS WIDE ML / TF RISK ASSESSMENT AND CUSTOMER RISK SCORING

35. Virtual currencies carry a significant ML/TF risk, as there is little to no prevention controls and measures at global level. In addition, virtual currency transactions may be anonymous and can allow individuals to purchase goods and services without possibility of identification. Supranational risk assessment report of EU considers the risk posed by virtual currency activities as significant. This leads to the Company's need to adapt its risk assessment procedures accordingly.

36. In the business wide ML / TF risk assessment (hereinafter – ML/TF risk assessment), the Company will analyze potential threats and vulnerabilities to money laundering and terrorist financing to which the business is exposed.

37. When identifying whether there is higher risk of money laundering and/or terrorist financing the Company will assess at least the following:

- **customer risk factors:**

a) the business relationship of the customer is conducted in unusual circumstances without any apparent economic or lawful purpose,

b) the customer is resident in a high risk third country,

c) legal persons or entities without legal person status acting as asset-holding vehicles,

d) legal entity has nominee shareholders or issued bearer shares,

e) the ownership structure of legal person appears unusual or excessively complex given the nature of the legal person's business.

The risk assessment requires that the Company knows its customers and the nature of their business. This is not limited to identification process or record keeping, but it is about understanding customers, including their activities, transaction patterns, and how they operate.

In addition to customer identification processes, the Company understands the ongoing problem with virtual currency anonymity both in Lithuanian jurisdiction, as well as abroad. Since the regulation and technological means to survey and control virtual currency trade are still being researched and implemented, the Company will closely follow official recommendations and guidelines issued by state authorities (such as the Financial Crime Investigation Service).

- **product, service, transaction or delivery channel risk factors:**

a) virtual currency transactions may be anonymous and can allow individuals to purchase goods and services without possibility of identification ,

b) business relationship or transactions are established or conducted without the physical presence,

c) payments are received from unknown or unassociated third parties,

d) products and business practices, including delivery mechanism, are new and new or developing technologies are used for both new and pre-existing products.

The Company will identify products and services or combinations of them that may pose an elevated risk of money laundering or terrorist financing. Products and services that can support the movement and conversion of assets into, through and out of the financial system pose a high risk.

- **geographical risk factors:**

a) countries identified, on the basis of data of reports or similar documents by the Financial Action Task Force (FATF) or a similar regional organization, as having significant non-compliances with international requirements in their anti-money laundering and/or counter financing of terrorism systems,

b) countries identified, on the basis of data by governmental and universally recognized non-governmental organizations monitoring and assessing the level of corruption, as having significant levels of corruption or other criminal activity,

c) countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations,

d) countries provide funding or support for terrorist activities or have designated terrorist organizations operating within their country.

Certain geographic locations potentially pose an elevated risk for money laundering and terrorist financing.

38. The ML / TF risk assessment results may identify increased-risk situations for which additional risk mitigation controls and monitoring may be required.

39. The ML / TF Risk assessment is a written document based on statistical data which outlines risk mitigation controls in place and their effectiveness so that residual risk can be assessed for each risk identified.

40. The results of the ML / TF risk assessment and remediation plan are communicated to the Management Board who will need to approve remediation plan and assign responsible people to carry it out.

41. ML / TF risk assessment is carried out every year.

42. Customers are classified into different risk levels by following at least customer, product, service, transaction or delivery channel, and geographical risk factors as described in point 37. Customers are assigned low, medium and high risk, while prohibited risk customers are not accepted.

43. The customer risk scoring matrix is used for customer risk assessment purposes.

44. When a customer is identified as high-risk, they are subject to appropriate enhanced due diligence measures.

45. For new customers risk scoring is performed before entering into a business relationship. The Company performs risk scoring for existing customers during ongoing due diligence.

- **Risk Level Assessment Matrix**

Low	Moderate	High
Stable, known client / Return	Client who did up to 2 transactions with us	New client
The client is located in high tax rate jurisdiction	There is a moderate tax rate in the client's jurisdiction	There is very low tax rate in the client's jurisdiction
Whether the origin of the client’s assets or the source and origin of the funds used for a transaction can be easily identified		Whether the origin of the client’s assets or the source and origin of the funds used for a transaction can't be identified

very low amount of transaction up to 1K	Moderate amount of transaction 1-5K	amount of transaction above 5K
Whether the jurisdictions isn't involved apply legal provisions that are in compliance with the international standards of AML/CTF		Whether the jurisdictions involved apply legal provisions that are in compliance with the international standards of AML/CTF
The client is located in an area known to have low crime rate and included in international sanction lists	The client is located in an area known to have moderate crime rate and included in international sanction lists	The client is located in an area known to have high crime rate and included in international sanction lists
No transactions with high-risk geographic locations (CHB / recall)	Minimal transactions with high-risk geographic locations (CHB / recall)	Significant volume of transactions with high-risk geographic locations (CHB / recall)
Age of the client 22-45	Age of the client 45-70	Age of the client 70-80

Purpose Of The Risk Management Plan

Annual audit

A risk is an event or condition that, if it occurs, could have a positive or negative effect on a project's objectives. Risk Management is the process of identifying, assessing, responding to, monitoring, and reporting risks. This Risk Management Plan defines how risks associated with the project will be identified, analyzed, and managed. It outlines how risk management activities will be performed, recorded, and monitored throughout the lifecycle of the project and provides templates and practices for recording and prioritizing risks.

Risk management Procedure

Process

The project manager working with the project team and project sponsors will ensure that risks are actively identified, analyzed, and managed throughout the life of the project. Risks will be identified as early as possible in the project so as to minimize their impact. The steps for accomplishing this are outlined in the following sections

Risk Identification

Risk identification will involve, appropriate stakeholders, and will include an evaluation of environmental factors, organizational culture and the project management plan including the project scope.

Risk Analysis

All risks identified will be assessed to identify the range of possible project outcomes. Qualification will be used to determine which risks are the top risks to pursue and respond to and which risks can be ignored.

Qualitative Risk Analysis

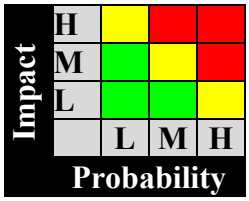
The probability and impact of occurrence for each identified risk will be assessed by the project manager, with input from the project team using the following approach:

Probability

- High – Greater than *<70%>* probability of occurrence
- Medium – Between *<30%>* and *<70%>* probability of occurrence
- Low – Below *<30%>* probability of occurrence

Impact

- High – Risk that has the potential to greatly impact project cost, project schedule or performance
- Medium – Risk that has the potential to slightly impact project cost, project schedule or performance
- Low – Risk that has relatively little impact on cost, schedule or performance



Risks that fall within the RED and YELLOW zones will have risk response planning which may include both risk mitigation and a risk contingency plan.

Quantitative Risk Analysis

Analysis of risk events that have been prioritized using the qualitative risk analysis process and their affect on project activities will be estimated, a numerical rating applied to each risk based on this analysis, and then documented in this section of the risk management plan.

Risk Response Planning

Each major risk (those falling in the Red & Yellow zones) will be assigned to a project team member for monitoring purposes to ensure that the risk will not “fall through the cracks”.
For each major risk, one of the following approaches will be selected to address it:

- **Avoid** – eliminate the threat by eliminating the cause
- **Mitigate** – Identify ways to reduce the probability or the impact of the risk
- **Accept** – Nothing will be done
- **Transfer** – Make another party responsible for the risk (buy insurance, outsourcing, etc.)

For each risk that will be mitigated, the project team will identify ways to prevent the risk from occurring or reduce its impact or probability of occurring. This may include prototyping, adding tasks to the project schedule, adding resources, etc.
For each major risk that is to be mitigated or that is accepted, a course of action will be outlined for the event that the risk does materialize in order to minimize its impact.

Risk Monitoring, Controlling, And Reporting

The level of risk on a project will be tracked, monitored and reported throughout the project lifecycle.

Tools And Practices

A Risk Log will be maintained by the project manager and will be reviewed as a standing agenda item for project team meetings.

risk management plan approval

The undersigned acknowledge they have reviewed the **Risk Management Plan** for the Audit project. Changes to this Risk Management Plan will be coordinated with and approved by the undersigned or their designated representatives.

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____

Signature: _____ Date: _____

Print Name: _____

Title: _____

Role: _____

Impact Scoring Table				
Consequenece	low	Medium low	Medium	High
Liqudity risk (Financial Loss)	Expensees that were not planned 10,000 EUR	merchants's fraud 10,000 EUR -50,000 EUR	Penalties by bank regulation 50,000 -100,000 EUR	bank acquirer went bankrupt or disappeared with our settlments funds 100,000 EUR and up
Stratgic risk	the employees don't understand the company's policies and business plan	Competitive develop new payment solition before us	Political events & conditions can disturb to the merchnats activities and impact all the payment industry	changes in customer preference
Reputation risk	Employees arguing with customer , the event was reach with other merchants	Competitive create rumors regarding the company cause bad reputation	Bad reviews from the merchant can cause that the merchant will stop working	An employee get bribery or other benefits from merchant
Operational risk	lost / leaving of stasff management level non management level	An employee violates the company policy	Settlment funds were sent to wrong merchant (Human mistake)	virus attack in the system ,cause by employee using US personal flash in the company PC
Legal risk	Threat of bank policy change which require small change in the company	Threat of change the FMA regulation change for all the payment industry and will impact the company	The merchants were onbaord without the correct AML & compliance policy	Contractual risk , The merchants don't work according to our banks and the FMA compliance policy , it means they act not
Information Techology	Human error, incorrect data processing , careless data disposal	Hardware and Software failure	Cyber attach and the system complete shut down over 1 hour	nature force major , no electricity all the area for long time

	The threat's source is highly motivated and sufficiently capable, and controls that prevent the vulnerability from being exercised are ineffective.
	The threat's source is motivated and capable, but controls are in place that may impede a successful exercise of the vulnerability.
	The threat's source lacks motivation or capability, and controls are in place to prevent or significantly impede the vulnerability from being exercised.

6 risk Categories :

1. Strategic risk
2. Operational
3. Reputaion
4. Legal
5. Liquidity
6. Information technology

VI. IDENTIFICATION AND VERIFICATION OF THE CUSTOMER AND THE BENEFICIAL OWNER

46. Identification of the customer and beneficial owner means:

46.1. determining whether the customer is acting on his own behalf or under control,

46.2. if the customer is acting through a representative, identifying customer's representative,

46.3. identifying customer (natural person),

46.4. identifying customer (legal entity),

46.5. identifying customer's (legal entity) beneficial owner (full name, personal code or date of birth, nationality, ownership %),

46.6. collecting information about customer's (legal entity) director (full name, personal code or date of birth, nationality)

46.7. collecting information on the ownership and management structure of customer legal entity, nature of its business,

46.8. collecting information on the purpose and intended nature of the business relationship of a customer (natural or legal person),

46.9. verifying the identity of the customer and the beneficial owner on the basis of documents, data or information obtained from reliable and independent sources.

47. When there is no possibility to fulfil the customer and beneficial owner identification requirements – suspension of transactions, refusal to establish or termination of business relationship.

48. The Company will take measures to identify the customer and the beneficial owner as well as verify their identity:

48.1. prior to establishing business relationship. The creation of a deposit wallet of virtual currencies is not a business relationship if no more than one transaction, operation, deposit or withdrawal has taken place in that wallet and the amount is less than EUR 700 or currency/ virtual currency equivalent,

48.2. before,

- executing occasional virtual currency exchange transactions or operations in virtual currency with funds equal to or above EUR 700 or currency/virtual currency equivalent.
- occasional depositing or withdrawing of virtual currency amounting to or above EUR 700 or currency/virtual currency equivalent.
- transaction is carried out in one or more interrelated transactions (the value of the virtual currency being determined at the time of the monetary transaction or operation) unless the customer and beneficial owner have already been identified.

48.3. when there are doubts about the veracity or authenticity of the previously obtained identification data of the customer and the beneficial owner,

48.4. in any other case when there are suspicions that an act of money laundering and/or terrorist financing is, was or will be carried out.

49. The Company will carry out customer's and beneficial owner's identification by applying a risk-based approach using:

- customer identification tools and customer due diligence (CDD) procedures,
- additional customer authentication tools and procedures for enhanced due diligence (EDD),
- simplified customer identification tools and procedures for simplified due diligence (SDD).

50. The Company will not open anonymous accounts or accounts under obviously fictitious names and will not open accounts or otherwise start business relationships without requesting customer to provide data confirming his identity or if there is a reasonable suspicion that the provided data is fake or falsified.

51. In case the Company is unable to meet the requirements set out in point 50, the Company will carry out the money laundering and/or terrorist financing threat assessment. After detecting the risk of money laundering and/or terrorist financing (ML/TF), the Company will report the suspicious monetary operation or transaction to the FCIS.

CUSTOMER DUE DILIGENCE

52. The purpose of customer due diligence (CDD) is to collect, process, verify and keep the information about the customers to minimize possible and/or potential ML/TF risks.

53. For all customers identification procedure must be completed prior entering into business relationship and it is necessary to complete the following steps:

53.1. perform identification and verification – identify and verify the identity of the customer and related parties.

53.2. screen all customers and related parties against various EU, UN and OFAC Sanctions Lists.

53.3. screen all customers and related parties to determine if the customer is a PEP or if there are any PEP associated with the customer.

53.4. verify as many customer details as possible in the public registers and perform open-source search for all other relevant information.

53.5. check the collected information.

53.6. perform customer risk scoring.

54. When conducting identification procedure, collect natural person's identity document – passport, identity card, driver's license (issued in the European Economic Area and complying with the requirements set out in Annex I of Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licenses (Recast)) or residence permit issued in the Republic of Lithuania which contains the following data:

a. name/names,
b. surname/surnames,
c. personal number (in the case of an alien – date of birth (where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification), the number and period of validity of the residence permit in the Republic of Lithuania and the place and date of its issuance (applicable to aliens),
d. photograph, (selfie with ID)
e. signature (except for the cases where it is optional in the identity document),
f. citizenship (in the case of a stateless person – the state which issued the identity document).
g. declaration of buying crypto currency
h. selfie with the declaration of buying crypto currency
i. source of funds (in total over Eur 10K)

55. When the collected identity document does not contain the natural person's citizenship, the Company obtains information on the natural person's citizenship directly from official registers and in the absence of such records – from the customer.

56. When conducting identification procedure, collect legal entity's registration certificate or copies thereof with a notarial certificate, confirming authenticity of the document's copy, which contain the following data:

a. name,
b. legal form, registered office/address, address of actual operation,
c. registration number (if such number has been issued),
d. an extract of registration and its date of issuance.

57. The identity of the legal person's representative shall be established in the same manner as the identity of the customer that is a natural person.

58. Identification information of the customer natural person, legal entity and its representative must be verified using reliable and independent sources, i. e., using real-time verification on ID document, obtaining a registration certificate directly from the state register.

59. The customer must provide information about the legal person's director:

a. name, surname,
b. personal number (in the case of an alien – date of birth (where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification),
c. citizenship (in the case of a stateless person – the state which issued the identity document).

SIMPLIFIED DUE DILIGENCE

60. Simplified due diligence (SDD) is the minimum level of due diligence that must be applied to the customer.

61. SDD may be carried out when the Company assesses customer's risk as Low and one of the following conditions are fulfilled,

a. Customer is a listed company (EU or equivalent).
b. Customer is a government or municipality institution.

62. When applying SDD, Company must,

- For individual customers – obtain name, surname and personal number.
- For business customers – obtain name, legal form, registered office/address, address of actual operation, registration number (if such number has been issued).
- Get customer's first top-up from his/her bank, payment or electronic money account in EU or third country having same level as Lithuanian AML requirements.
- Ensure ongoing monitoring of the business relationship.
- Regularly check if the customer is still eligible for SDD.

63. SDD is not permitted if there are mandatory conditions to perform EDD or CDD.

ENHANCED DUE DILIGENCE

64. Enhanced due diligence (EDD) refers to the situations where a customer presents higher risk of ML/TF and standard evidence of identity may be insufficient. Additional information needs to be obtained to assist with the customer approval and monitoring processes.

65. EDD involves objective, rigorous, and thorough research that provides a greater view of the customer's profile and the actions required to mitigate higher risks.

66. Enhanced due diligence (EDD) shall be conducted under the following circumstances:

- when transactions or business relationships are conducted with politically exposed persons (PEP).
- when business relationships are established with, or transactions carried out with natural persons or legal entities from high-risk third countries identified by the European Commission.
- when transactions or business relationships are conducted with natural persons or legal entities from countries identified by the Financial Action Task Force (FATF) as high risk.

- when the Company assesses customer's risk as high using its risk scoring matrix.

67. When transactions or business relationships are conducted with PEPs, the Company must:

- Have PEP procedure in place.
- Obtain approval from the senior manager to establish or continue business relationships with such costumers.
- Identify and verify customer's source of wealth and (or) funds involved in a business relationship or transaction.
- Carry out a constant enhanced monitoring of the business relationship with these customers.

68. When business relationship is established with or transactions carried out with natural persons or legal entities from high-risk third countries identified by the European Commission, the Company must:

- obtain additional information about the customer and the beneficial owner.
- obtain additional information on the intended nature of the business relationship.
- obtain information on the source of wealth and (or) funds of the customer and beneficial owner.
- obtain information on the reasons for anticipated or completed transactions.
- obtain approval from senior management to establish or continue business relationships with these customers.
- conduct enhanced ongoing monitoring of business relationships with these customers by increasing the number and timing of controls to be applied and selecting the types of transactions that will require further investigation.
- ensure that the first payment by a customer is made from that customer's bank, payment, or electronic money account in European Union or in a third country which has equivalent AML requirements and supervision.

69. When transactions or business relationships are conducted with natural persons or legal entities from countries identified by the FATF as high risk **OR** the Company assesses customer's risk as high using its risk scoring matrix, the Company must:

- Obtain senior management approval for establishing or continuing business relationships with these customers.
- Identify and verify customer's source of wealth and (or) funds involved in a business relationship or transaction.

- Conduct enhanced ongoing monitoring of business relationships with these customers.
- Apply additional measures at the discretion of The Head of AML (MLRO):
    - ➢ obtain additional information about the customer and the beneficial owner.
    - ➢ obtain additional information on the intended nature of the business relationship.
    - ➢ obtain information on the reasons for anticipated or completed transactions.
    - ➢ ensure that the first payment by a customer is made from that customer's bank, payment or electronic money account in European Union or in a third country which has equivalent AML requirements and supervision.

VII. SANCTIONS AND POLITICALLY EXPOSED PEOPLE (PEP) SCREENING

70. The Republic of Lithuania follows the measures taken by the European Union, United Nations and the United States which are implemented through the Law on the Implementation of Economic and Other International Sanctions. These measures include a list of individuals and entities who/which are subject to sanctions. The Ministry of Foreign Affairs coordinates the implementation of international sanctions in Lithuania and provides information about it.

71. The Company must check if customers, representatives of the customers or the beneficial owners are not on the list of persons subject to international financial sanctions.

72. A check against sanctions lists shall be carried out during identification stage. All customers are continuously screened for sanctions for the length of the business relationship and at the time of transactions.

73. The Company will follow Instructions for the supervision of the appropriate administration of International Financial Sanctions in the field of Regulation of the Financial Crime Office under the Ministry of the Interior of the Republic of Lithuania approved by the FCIS Director on October 20th 2016 by Resolution No. V-273 "On the approval of the supervisory instructions of the Financial Crimes Investigation Service under the Ministry of the Interior of the Republic of Lithuania in the field of regulation of the proper implementation of international financial sanctions", therefore, the Company must:

- provide information about the implementation of financial sanctions to the FCIS and the Ministry of Foreign Affairs of the Republic of Lithuania,
- provide the FCIS with all data necessary for monitoring,

- appoint employee(s) who would organize the implementation of financial sanctions, be in charge of termination of disposal of accounts, regular update of the list of entities which are under financial sanctions, reporting to the FCIS and other authorities responsible for monitoring of the implementation of international sanctions.

74. If a positive match is determined, the Head of AML (MLRO) must:

- Freeze customer's account and (or) stop the transaction,
- Within 2 business days via email inform FCIS (sankcijos@fntt.lt) and the Ministry of Foreign Affairs (urm@urm.lt).
- Wait for further instructions from FCIS and/ or the Ministry of Foreign Affairs.

75. The Company will not establish business relationships with customers subject to international financial sanctions.

76. The Company must check if customers, representatives of the customers or the beneficial owners are not PEP.

77. A PEP self-declaration form is included in each KYC questionnaire and to verify information obtained from customers all names will be searched through credible sources of commercially or publicly available information.

78. PEP status itself does not incriminate individuals or entities. It does, however, put the customer or legal entity into a high-risk category and makes it subject to EDD.

79. Such customers remain high-risk for at least one year after officially seizing to be a PEP.

80. PEP screening is an ongoing process for all customers for the length of the business relationship.

VIII. ONGOING DUE DILIGENCE, TRANSACTION MONITORING AND SAR REPORTING

81. Ongoing monitoring is an activity that comprises scrutiny of transactions undertaken throughout the course of a business relationship to minimize its exposure to financial crime risks as well as ensuring that the data or information on the Customer is kept up to date.

82. Ongoing monitoring is comprised of:

82.1. Transaction Monitoring (TM):

- Real-time Monitoring
- Retrospective Monitoring
- Screening blockchain transactions

82.2. Ongoing Due Diligence (ODD):

- Periodic Ongoing Due Diligence
- Event-driven Ongoing Due Diligence.

83. Once a business relationship is established with a customer, the Company will monitor the business relationship to ensure that the transactions executed correspond to the information held by the Company about customer, his business, risk nature and source of funds.

84. The Company assesses each customer's risk score and assigns risk rate. The risk rate of the customer determines how frequently the Company will review each business relationship and how frequently that business relationship information is updated. All customer relationships need ongoing due diligence, but high-risk customers will be monitored more frequently.

85. The scheduled frequency of review:

- high-risk customers will be reviewed every six months,
- medium risk customers will be reviewed annually, and
- low-risk customers will be reviewed every two years.

86. ODD of each business relationship is intended to:

- detect suspicious activity that must be reported,
- keep customer KYC, the purpose and intended nature of the business relationship, and beneficial ownership information up to date,
- re-assess the level of risk associated with the customer's transactions and activities,
- determine whether the transactions or activities are consistent with the information previously obtained about the customer, including the risk scoring,
- understand customer's activities over time so that any changes can be measured to detect high risk.

87. These requirements do not need to follow the same timeframe, as long as high-risk customers are monitored more frequently and with more scrutiny than low-risk customers. Monitoring high-risk situations may include measures such as:

- reviewing transactions based on an approved schedule that involves management sign-off,
- developing reports or performing more frequent review of reports that list high-risk transactions, flagging activities or changes in activities from expectations and elevating concerns as necessary,
- setting business limits or parameters regarding accounts or transactions that would trigger early warning signals and require mandatory review,
- reviewing transactions more frequently against suspicious transaction indicators relevant to the relationship.

88. The Company monitors customers' transactions on an on-going basis and has instituted real-time monitoring of all customer transactions as well as retrospective monitoring of customer transactions fitting a specific risk criterion provided by the FCIS.

89. The company applies a risk-based approach to transaction monitoring which includes wide manual controls, staff vigilance and use of automated scenarios and rule-based solutions. In high-risk and very high-risk customer relationships the Company chooses to apply enhanced monitoring measures.

90. Triggers which can be used to generate alerts in respect of transactions and customers which in turn need to be reviewed and checked include:

90.1. The size of particular transaction

90.2. Volume and number of transactions

90.3. Frequency of transactions in particular period

90.4. Geographies of activity - transactions received/sent from high-risk countries with no reasonable explanation

90.5. Structuring of transactions to avoid dealing with identification requirements or regulatory record- keeping and reporting thresholds

90.6. High increase in activity

90.7. Networking rules- many to one and one to many scenarios

90.8. Transit accounts

91. Suspicious monetary operations or transactions shall be identified:

- in accordance with the criteria for the identification of suspicious monetary transactions or transactions approved by Resolution No. V-240 of December 5th of 2014 of the Director of Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania "On the Approval of the List of Criteria for Money Laundering and Suspicious or Unusual Monetary Operations or Transactions Identification", for example,
    - During the identification process, the potential customer avoids providing the information necessary to establish his identity
    - By dividing a monetary operation or transaction into several smaller units, the customer seeks to avoid identification
    - Monetary operations or transactions of a non-profit institution or organization do not correspond to the types of activities specified in its founding documents
    - Monetary operations or transactions are carried out with individuals and legal entities from high-risk regions

- noting the activities of customers which, by their nature, may be related to money laundering and/or terrorist financing,
- conducting customer’s and beneficial owner’s identification,
- conducting ongoing monitoring of the customer's business relationship, including the investigation of transactions that have occurred during that relationship.

92. When a suspicious monetary operation (SAR) or transaction is detected, a documented investigation must be completed, that operation or transaction must be suspended, and a report made to the FCIS within three business hours after suspicious activity is completed and it is decided to report it. There is no minimal threshold or limit for such a report.

93. A SAR must be submitted to the FCIS immediately when the Company receives information that the customer intends or will attempt to perform a suspicious monetary operation or transaction.

94. Once SAR is reported to the FCIS, they are required to respond within ten working days. If the FCIS requests further information, then a response to that request must be provided immediately.

95. Recommended structure of SAR provided to the FCIS:

- Start the SAR description with the client's (legal and/or natural person) data (details), exact name, surname, personal identification number or year of birth, citizenship; exact company name, code, registration address, manager, beneficial owner. Other details of the client can be provided in the attachments if they are not directly related to the description of the situation and/or suspiciousness criteria.
- Provide exact description of the situation, date of the transaction, (duration of the transaction, if it is a transaction lasting a certain time), place (territory, city, country), other parties to the transaction (legal or natural persons), subject of the transaction (goods, services), other facts or circumstances related to the transaction (e.g. product quality certificate, customs procedures, previous SAR provided for the same customer which may be related to this notification, etc.).
- It is recommended to seek consistency, clarity of description, to avoid unclear or incomprehensible abbreviations and grammatical errors.
- In the description of the submitted SAR, it is necessary to indicate what suspicion arose regarding the possible illegal act of the customer, what suspicion criteria were established during the Company's internal investigation.
  NOTE, the list of criteria for identifying suspicious transactions or operations approved by the order of the director of the FCIS is not exhaustive. During the internal investigation, the Company may establish new criteria for a suspicious transaction, but they must be described and motivated.
- Together with the SAR submit all documents or other data in the possession of the Company on which the description of the said SAR was based, as well as account statement, incorporation documents of a legal entity, customer questionnaire

(KYC), identity document of the customer or his representative, proof of Source of Wealth/Funds, correspondence with the customer, photo or video from ATMs, if funds received from a suspicious transaction were cashed, IP addresses etc.
NOTE, all documents are submitted only in electronic format (PDF, Excel, Word, etc.).

- Indicate the contact details of the MLRO who submitted the SAR, e-mail and telephone number for possible feedback.
- In the feedback platform of the FCIS, the Company is informed about the quality of the SAR received. If necessary, on this platform, the Company may be asked to provide additional documents or data that are necessary for the analysis of the received SAR.

96. It is a criminal offence for anyone, following a disclosure to a nominated officer or to the appropriate institution, to do or say anything that might either "tip off" another person that a disclosure has been made or prejudice an investigation. When customer account is the subject of a SAR, there must be taken careful steps while communicating with customer and additional advice should be taken from the Head of AML (MLRO) in order not to accidentally disclose investigative actions to the customer.

97. The Company shall notify the FCIS of the customer's identity data and information on the executed virtual currency exchange transactions (virtual currency purchase or sale in decree currency) or virtual currency transactions (virtual currency asset settlements) if the value of a monetary operation or transaction is equal to or greater than EUR 15 000 or currency/virtual currency equivalent, whether the transaction is carried out in the context of one or more related monetary operations. The value of the virtual currency is determined at the time of the monetary operation or transaction.

98. In the event that a customer's monetary operation or transaction meets the requirements of both points 92 and 97 of this Policy, the Company shall submit notice of suspicious monetary operation or transaction and notification of executed virtual currencies exchange operation or transactions in virtual currency where the value of such monetary operation or transaction is equal to or greater than EUR 15 000 or currency/virtual currency equivalent, whether or not the transaction is executed in the context of one or more related monetary transactions to the FCIS.

IX. EMPLOYEE TRAINING

99. The Company has a yearly training program for all employees and other individuals who act on behalf of the Company to make sure that those who have contact with customers, who see customer transaction activity understands the reporting, customer identification and record keeping requirements.

100. All new employees of the Company are required to complete anti-money laundering and terrorist financing compliance training within their induction training period when they

join the Company. All employees will be enrolled and undertake the comprehensive and regular Company-wide anti-money laundering and counter-terrorist financing training within their first six months of employment with the exception applicable to the employees who are directly involved in application of the AML/CTF measures (such as the Head of AML (MLRO)) who must be introduced to the procedures of the Company before they will start performing functions with the relation to AML/CTF.

101. The Head of AML (MLRO) is responsible for ensuring that everyone is periodically informed of changes in AML/CTF legislation, policies and procedures, and current developments in money laundering or terrorist activity financing schemes particularly relevant to their jobs. To ensure employee training is kept up to date, all existing employees will receive follow up training on new and existing AML/CTF and regulatory requirements on a regular basis (at least within one year of their last training).

102. A log of assigned and completed training materials shall be kept up to date by the Head of AML (MLRO) and on file for five years (e. g. extract or download of training logs).

103. Relevant compliance training is for all employees and relevant outsourced service providers. This includes those persons in sales and in senior management and others who have responsibilities under the AML/CTF compliance regime, such as information technology officer and other staff responsible for designing and implementing electronic or manual internal controls. The Head of AML (MLRO) will review functions and arrange to provide suitable and customized training.

104. The Company's training will include at a minimum:

- General background and history pertaining to money laundering controls, including the definitions of money laundering and terrorist financing, why criminals do it, and why stopping them is important.
- Legal framework on what AML/CFT laws apply to institutions and their employees.
- Penalties for AML/CFT violations, including criminal and civil penalties, fines, jail terms, as well as internal sanctions, such as disciplinary action up to and including termination of employment.
- Internal policies, such as customer identification and verification procedures and policies, including Customer Due Diligence (CDD), Enhanced Due Diligence (EDD) and Ongoing Due Diligence (ODD).
- Review of the internal AML/CFT and sanctions risk assessments.
- Legal record keeping requirements.
- Suspicious transaction monitoring and reporting requirements.
- How to react when faced with a suspicious client or transaction.

- How to respond to customers who want to circumvent reporting requirements.
- Duties and accountability of employees.
- Maintaining confidentiality with AML/CFT-related matters.
- AML/CFT trends and emerging issues related to criminal activity, terrorist financing and regulatory requirements.
- Money laundering schemes (preferably cases that have occurred at the company or at similar institutions), including how the pattern of activity was first detected, its impact on the institution, and its ultimate resolution.

105. Certain employees, such as those in AML/CTF compliance, customer services and operations, require types of specialized additional training which will be provided either through external services or internally. The training program will be reviewed and updated to reflect requirements.

X. RECORD KEEPING

106. Accurate record keeping is imperative to evidence all financial crime risk management related activities and decisions as well as compliance with the AML. The Company must keep the following records,

Customer Identification Records:

- customer's identity documents and beneficial owner data,
- all risk scoring records as well as the customer risk profile,
- KYC questionnaire,
- all records related to ODD.

Transactions records:

- a log containing transactional data during business relationship,
- internal suspicious activity investigations,
- a log of SAR reporting,
- a log of virtual currency exchange transactions or transactions in virtual currency, if such monetary transaction or value of transaction is equal or greater than EUR 15 000 or currency/virtual currency equivalent, it is not important if transaction is executed through one or more related monetary transactions,
- a log of due to ML/TF reasons terminated business relationship.

Other records:

- evidence of the training programs on money laundering/terrorism financing prevention whether in-house or external,
- other records if required under the AML law of Lithuania as well as other legal acts related to the prevention of money laundering/terrorism financing,

107. The data in the registration logs must be entered in a chronological order, without delay, but not later than within 3 working days after the execution of the transaction.

108. All AML/CTF related records must be stored electronically, in a readily accessible and retrievable format and made available without delay upon request from the Head of AML (MLRO) or any relevant external bodies, including competent authorities. The Company will retain AML/CTF related records electronically.

109. Time period of record keeping:

1.	Log of Submitted SARs	To be kept for 8 years after terminating business relationship
2.	Log of virtual currency exchange and transactions equal or greater than EUR 15 000 or currency/virtual currency equivalent	
3.	Log of all customer transactions	
4.	Log of business relationships terminated due to ML/TF reasons	
5.	Copies of ID documents, identification information and KYC information	
6.	Virtual currency wallet address together with owner's identity information	
7.	Correspondence with customer	To be kept for 5 years after terminating business relationship
8.	Supporting documents obtained from customer	To be kept for 8 years after completing transaction
9.	Internal investigation records of suspicious transactions	To be kept for 5 years
10.	Training log and related documents	To be kept for 5 years after the end of training

110. All The Head of AML (MLRO) reports to the General manager and the Board will be kept indefinitely.

111. The time limits for record keeping may be extended additionally for no longer than two years upon a reasoned instruction of a competent authority.

112. The registration logs are kept in accordance with Resolution No. V-129 of September 4th of 2017 of the Director of Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania “On the Approval of the Rules for Keeping the Register of Suspicious or Unusual Monetary Operations and Transactions of the Customer and Identification of the Criteria that Characterizes Large-Scale Permanent and Regular Monetary Operations“.

113. By March 31 of each year, the Company will provide information and reports to the FCIS on the implementation of the AML/CTF measures according to the Information Description approved by the FCIS.

CLOSING REMARKS

114. Adherence to this AML/CTF policy and its implementing procedures is a shared responsibility of the management and all the staff of the Company.

Appendix A

SUSPICIOUS TRANSACTION REPORT

For Money Laundering and Funding of Terrorism

Date ☐☐☐☐☐☐ Report Ref. No. ☐☐☐☐☐☐☐☐☐☐

Check appropriate box: ☐ Initial Report ☐ Supplemental Report

Previous connected reports: Ref. No. _____ Ref. No. _____

Part 1: Subject of Report

Full Name of Suspect (including aliases and/or nickname/s:	

Identification: Type and document number (If available, copy to be attached to this report):			
☐ Identity Card	☐ Passport	☐ Asia Payment Services Number	☐ Other – Specify
No. _____	No. _____	No. _____	_____

Expires: _____	Expires: _____	Expires: _____	Expires: _____
Address:			
Date of Birth / Registration:			
Occupation / Nature of Business:			
Nationality / Country of Incorporation:			
Date when Business Relationship was established:			
Type of Products (Accounts, Policies, Usernames, etc.) held with institution, if any:	(One product per box)	(One product per box)	(One product per box)
Product/Relationship (Accounts, Policies, Usernames, etc.) Number			
Date of Opening/Closing of Product (Account, Policy, etc.,)			

Balance as at report date:			
Name of the MLRO (in block letters)		Signature of the MLRO	

Part 2: Suspicious Transaction/ (Activity)

Date	Amount	Source

Explanation/description of suspicious transaction /activity

The STR should be described in a complete and clear manner. All facts should be given in a chronological order including what is unusual, irregular or suspicious about the transaction/activity being reported. All relevant information used by the MLRO supporting documentation that is likely to assist the FMA in its analysis should be attached to this report. **(Annex additional sheets if required.)**

List of Documents attached:

Name of the MLRO (in block letters)	MLRO'S Signature

Apendix B

Uppex – declaration of buing crypto currency

Declaration of Deposit

I hereby confirm that the below transactions were done solely by me via Uppex.com website for the purpose of buying crypto currency.

I certify that I am the authorized bank account or credit/debit cardholder. In case of a joint account, I authorize the account holder to use my card or bank account. By submitting these payments to the system, I am aware that the rate of the exchange, and all subsequent fees for the transaction, will be determined by Uppex.com at the time of execution and no refunds or cancellation of the transaction will be permitted after it has been approved. I also agree to all Terms and Conditions of Uppex.com. I also declare I made the purchase by myself, and not for third party

Bank Wire Transfer:

Date of Deposit (dd/mm/yyyy)	Amount and Currency	Signature

Bank Name:
Bank Address:
ABA Routing # (US Banks):
SWIFT Code and/or BIC:
IBAN:
Account Name:
Account Holder’s Address:
Account Number:
Additional Information:

Client's crypto E-Wallet Address:_____