«APPROVED»

CEO LLC «COINPAY»

_____KIM A.R

November 04, 2024

AML & RISK MANAGEMENT POLICY OF LLC «COINPAY»

CONTENTS

I. GENERAL PROVISIONS

1.1 Internal Control, Anti-Money Laundering, and Risk Management Policy (hereinafter referred to as the Policy) is aimed at regulating the activities of LLC "COINPAY" as a crypto shop for buying and selling cryptocurrencies. The Policy sets forth the internal procedures, systems, and control mechanisms designed to ensure high standards of fraud prevention, compliance with applicable laws, and effective risk management across all aspects of our operations. The Policy aims to promote a culture of compliance and integrity, ensuring that all activities are conducted in accordance with Uzbekistani laws and international best practices related to Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT). It outlines measures to identify, assess, and mitigate risks associated with money laundering, terrorist financing, fraud, and other illegal activities. This Policy applies to all partners, directors, employees, and consultants of LLC "COINPAY," regardless of the nature of their contractual relationship with the company. All personnel are required to familiarize themselves with and adhere to the provisions of this Policy.

1.2 LLC "COINPAY" reserves the right to amend this Policy at its discretion. In the event of any changes: Clients will be notified of amendments through official communication channels, including email notifications and updates on our website, at least 15 days prior to the changes taking effect; Continued use of our services after the effective date of the amended Policy constitutes acceptance of the changes. If a client does not accept the modified Policy, they are advised to cease using our services immediately. By implementing this Policy, LLC "COINPAY" is committed to:

- Upholding the highest standards of ethical conduct and regulatory compliance.
- Protecting the interests of our clients, stakeholders, and the financial system as a whole.
- Continuously improving our internal controls and risk management practices to adapt to evolving risks and regulatory requirements.

1.3 This Policy is drafted in accordance with the following provisions:

1.2.1 "Rules for the operation of a crypto shop" (appendix to the order of the director of the National Agency for Prospective Projects of the Republic of Uzbekistan dated September 29, 2022, No. 43, registered by the Ministry of Justice on October 31, 2022, No. 3395); Establishes operational standards, procedures, and requirements for crypto shops engaged in buying and selling cryptocurrencies

1.2.2 "Regulation on the procedure for licensing the activities of service providers in the field of circulation of crypto assets" (Appendix No. 1 to the order of the Director of the National Agency for Prospective Projects of the Republic of Uzbekistan dated July 14, 2022, No. 32, registered by the Ministry of Justice on August 15, 2022, No. 3380); Outlines the licensing procedures, compliance obligations, and oversight mechanisms for service providers dealing with crypto assets.

1.2.3 "Rules for trading crypto assets on a crypto exchange" (appendix to the order of the Director of the National Agency for Prospective Projects of the Republic of Uzbekistan dated July 18, 2022, No. 33, registered by the Ministry of Justice on August 15, 2022, No. 3379); Defines the regulatory framework for trading activities on crypto exchanges, including trading protocols and customer protection measures.

1.2.4 "Internal control rules for combating the legalization of proceeds from criminal activities, financing of terrorism and financing of proliferation of weapons of mass destruction for persons engaged in activities in the field of circulation of crypto assets" (Resolution of the Director of the National Agency for Prospective Projects of the Republic of Uzbekistan dated June 8, 2021, No. 3 and the Department for Combating Money Laundering dated June 7, 2021, No. 16, registered by the Ministry of Justice on June 9, 2021, No. 3309); Provides guidelines for establishing internal controls to prevent money laundering, terrorist financing, and proliferation financing within the crypto asset sector.

1.2.5 Other applicable regulatory and legislative acts. Encompasses any other relevant laws, regulations, directives, or guidelines issued by the Republic of Uzbekistan that are applicable to the company's operations, including future amendments and updates.

1.4 The terms used in this Policy have the following meanings:

List - a list of individuals involved or suspected of involvement in terrorist activities or the proliferation of weapons of mass destruction, formed by a specially authorized state body based on information provided by state bodies combating terrorism, proliferation of weapons of mass destruction, and other competent authorities of the Republic of Uzbekistan, as well as information obtained through official channels from competent authorities of foreign states and international organizations.

NAPP - National Agency for Prospective Projects of the Republic of Uzbekistan.

Internal control - the activities of individuals engaged in activities in the field of circulation of crypto assets, aimed at proper customer verification, risk management of money laundering, financing of terrorism, and financing of proliferation of weapons of mass destruction, identification of suspicious transactions, as well as transactions involving individuals involved or suspected of involvement in terrorist activities, financing of terrorism, or financing of proliferation of weapons of mass destruction.

Proper customer verification - the verification of the customer and the persons on whose behalf they are acting, identification of the beneficial owner of the customer, as well as conducting ongoing monitoring of the business relationships and transactions conducted by the customer to verify their compliance with the information about the customer and their activities.

States not participating in international cooperation in combating money laundering, financing of terrorism, and financing of proliferation of weapons of mass destruction - states and territories identified in official statements of the Financial Action Task Force (FATF) as posing a threat to the international financial system and having strategic deficiencies in their systems for combating money laundering, financing of terrorism, and financing of proliferation of weapons of mass destruction.

Customer identification - establishing data about customers based on the documents provided by them, for the purpose of conducting proper customer verification.

An individual or entity involved or suspected of involvement in terrorist activities - a legal or natural person who participates or is suspected of participating in terrorist activities, a legal or natural person who directly or indirectly owns or controls an organization engaged in or suspected of engaging in terrorist activities, and a legal entity owned or controlled by a natural person or organization engaged in or suspected of engaging in terrorist activities.

An individual or entity involved or suspected of involvement in the proliferation of weapons of mass destruction - a natural or legal person identified by relevant resolutions of the United Nations Security Council and other international legal instruments recognized by the Republic of Uzbekistan, aimed at preventing the proliferation of weapons of mass destruction.

Responsible Employee: An individual designated by LLC "COINPAY" responsible for organizing and implementing internal control measures.

Public officials - individuals appointed or elected permanently, temporarily, or by special mandate, performing organizational and managerial functions and authorized to perform legally significant actions in legislative, executive, administrative, or judicial bodies, including military structures of foreign states or international organizations, as well as high-ranking officials of enterprises of foreign states, known politicians, and known members of political parties of foreign states (including former ones).

Internal control system - a set of actions by the responsible employee and individuals engaged in activities in the field of cryptocurrency asset circulation, aimed at achieving the goals and fulfilling the tasks defined by the legislation of the Republic of Uzbekistan and internal documents of LLC "COINPAY".

Specially authorized state body - the Department for Combating Economic Crimes at the General Prosecutor's Office of the Republic of Uzbekistan.

Risk - the risk of clients conducting operations for the purpose of laundering proceeds from criminal activities, financing terrorism, or financing the proliferation of weapons of mass destruction.

KYC (Know Your Client) - The process of verifying the identity of clients, assessing their suitability, and understanding the nature of their activities to prevent illegal activities.

KYT (Know Your Transaction) - The process of monitoring and analyzing transactions to detect and prevent money laundering, terrorist financing, and other financial crimes.

Beneficial Owner - A natural person who ultimately owns or controls a client or the person on whose behalf a transaction is being conducted, including those persons who exercise ultimate effective control over a legal entity or arrangement.

Client - Any individual or legal entity that uses or has used the services provided by LLC "COINPAY."

Crypto Asset - A digital representation of value that can be digitally traded, transferred, or used for payment or investment purposes, including cryptocurrencies.

Cryptocurrency - A type of crypto asset that uses cryptographic techniques for security and operates independently of a central bank.

Financial Action Task Force (FATF) - An intergovernmental organization that develops policies to combat money laundering, terrorist financing, and proliferation financing.

Money Laundering: The process by which criminals conceal the origins of illegally obtained money to make it appear legitimate.

Politically Exposed Person (PEP): An individual who is or has been entrusted with prominent public functions, including senior politicians, government officials, judicial or military officials, senior executives of state-owned corporations, and important political party officials.

Transaction: Any operation involving the exchange, transfer, or movement of crypto assets or funds.

Suspicious Transaction: A transaction involving crypto assets or funds that LLC "COINPAY" suspects is related to money laundering, terrorist financing, or proliferation financing.

Suspicious Transaction Report (STR): is an official document that LLC 'COINPAY' is legally obligated to submit to the specially authorized state body, such as the Financial Intelligence Unit (FIU) of the Republic of Uzbekistan, whenever there is a suspicion or reasonable grounds to suspect that a transaction or attempted transaction involves funds derived from illegal activities, is linked to terrorist financing, or otherwise violates laws related to Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT).

Customer Identification Program (CIP): is a mandatory process implemented by LLC 'COINPAY' to verify the identity of its customers when establishing a business relationship or opening an account.

Unauthorized Mining: Mining of cryptocurrencies without the necessary legal permissions or licenses required by law.

Shadow Settlements: Financial transactions conducted outside of official and regulated channels, often to conceal illicit activities.

Changers: Individuals or entities that illegally exchange crypto assets for fiat currency without proper authorization.

Shadow Banking System: A network of financial activities and intermediaries that operate outside of formal banking regulations.

Hawala: An informal method of transferring money without any physical movement of funds, often operating outside of regulated financial systems

1.5 The objectives of internal control:

The internal control system of LLC "COINPAY" aims to establish robust mechanisms to prevent and detect activities related to money laundering, terrorist financing, and proliferation financing. The objectives of the internal control system are as follows:

I.4.1 Effectively identifying and preventing operations involving funds or other property aimed at laundering proceeds from criminal activities, financing terrorism, and financing the proliferation of weapons of mass destruction.

I.4.2 Ensure strict adherence to all applicable laws, regulations, and guidelines of the Republic of Uzbekistan related to Anti-Money Laundering (AML), Counter Financing of Terrorism (CFT), and Counter Proliferation Financing (CPF).

I.4.3 Establish comprehensive CDD procedures, including Know Your Customer (KYC) and Know Your Transaction (KYT) processes, to verify the identity of clients and beneficial owners, and understand the nature and purpose of business relationships.

I.4.4 Prevent both intentional and unintentional involvement of the company and its employees in activities related to money laundering, terrorist financing, or proliferation financing

I.4.5 Identify, assess, document, and mitigate risks associated with money laundering, terrorist financing, and proliferation financing through the adoption of a risk-based approach

I.4.6 Conduct continuous monitoring of customer activities and transactions to detect unusual or suspicious patterns, and report such activities promptly to the specially authorized state body.

I.4.7 Provide regular training programs for employees to ensure they are knowledgeable about AML/CFT laws, internal policies, and procedures, thereby fostering a culture of compliance and ethical conduct.

I.4.8 Maintain accurate and complete records of all transactions, customer identification data, and due diligence information for the period stipulated by law.

I.4.9 Annually review and update internal control policies and procedures to ensure their effectiveness and compliance with evolving legal and regulatory requirements.

I.4.10 Safeguard the reputation and integrity of LLC "COINPAY" by demonstrating a strong commitment to legal compliance and ethical business practices.

1.6 **The main tasks of internal control are as follows**:

1.5.1 Taking appropriate measures to identify, assess, document, and mitigate its risks associated with money laundering, terrorist financing, and proliferation financing.

1.5.2 Implementing robust customer identification and due diligence procedures, including verification and regular updating of customer and beneficial owner data.

1.5.3 Identifying and verifying the identities of beneficial owners using all reasonable and available measures.

1.5.4 Conducting enhanced due diligence and ongoing monitoring of transactions involving former politically exposed persons (PEPs), their family members, and close associates.

1.5.5 Identifying and analyzing suspicious transactions in compliance with Uzbekistani legislation and LLC 'COINPAY' internal policies.

1.5.6 Promptly reporting identified suspicious transactions and providing all relevant documentation to the specially authorized state body.

1.5.7 Timely responding to requests for additional information and instructions from the specially authorized state body regarding the suspension of operations with funds or other property of clients.

1.5.8 Screening transaction participants against the official List to identify individuals or entities involved or suspected of involvement in terrorist activities or proliferation of weapons of mass destruction.

1.5.9 Maintaining the confidentiality of all information related to AML/CFT efforts, including client data and reports on suspicious activities.

1.5.10 Securing and retaining transaction records, customer identification data, and due diligence documentation for the legally required retention periods.

1.5.11 Providing timely and systematic provision of accurate information and materials necessary for decision-making to the management of LLC "COINPAY".

1.5.12 Establishing and maintaining a database of suspicious transactions and attempted transactions, including details of involved participants, and sharing this information with relevant authorities and, where legally permissible, with other crypto asset service providers in compliance with legislative requirements.

1.5.13 .Regularly screening the client database against the official List to identify individuals or entities associated with terrorist financing or proliferation financing

1.6 ESTABLISHMENT AND MAINTENANCE OF THE COMPLIANCE PROGRAM

It is the policy of LLC 'COINPAY' to prohibit and actively prevent money laundering, terrorist financing, and any activities that facilitate money laundering or the funding of terrorist or criminal activities, by ensuring full compliance with all applicable laws and regulatory requirements. LLC 'COINPAY''s Anti-Money Laundering (AML) policies, procedures, and internal controls are designed to ensure compliance with all applicable laws and regulations.

It will be the responsibility of the Compliance Officer and the Company's board of directors to review, adopt, and enforce this Policy in accordance with the laws described herein. The designated Compliance Officer will periodically review the AML and Risk Management Policy to ensure it remains current, effective, and legally compliant, updating it as necessary but at least once annually. Additionally, the Compliance Officer and the Company's Director have the individual and collective responsibility to promptly report to the Board of Directors of LLC 'COINPAY' and the National Agency for Prospective Projects (NAPP) any material concerns or violations related to the AML and Risk Management Policy that come to their attention. The Compliance Officer shall have sufficient independence, authority, and resources to carry out their duties effectively, including access to all relevant information within the company. LLC 'COINPAY' will ensure that all relevant employees receive adequate training on AML/CFT laws, regulations, and internal policies, to maintain a high level of compliance awareness throughout the organization. The Program will be subject to regular independent audits to assess its effectiveness and to identify areas for improvement.

II. RESPONSIBLE INDIVIDUALS FOR INTERNAL CONTROL

2.1 The internal control system of LLC 'COINPAY' is organized using a risk-based approach, considering the specific nature of the company's operations, primary business activities, relationships with agents and sub-agents, client base, and the associated risk levels of clients and their transactions.

2.2 The structure of the internal control system of LLC "COINPAY" is determined by the decision of the company's management and is approved by the order of the Compliance Officer of LLC "COINPAY".

2.3 The responsibilities of the designated internal control officer may be delegated to another qualified employee of LLC 'COINPAY' who has the necessary experience, has undergone appropriate training, and meets all regulatory requirements, ensuring that the effectiveness of internal controls is maintained.

2.4 The appointed responsible employee must have comprehensive knowledge and receive ongoing training in:

2.4.1 National legislation related to payments and payment systems, including all laws and regulations aimed at combating money laundering, terrorist financing, and proliferation financing.

2.4.2 International standards and best practices, such as those set by the Financial Action Task Force (FATF), for preventing money laundering, terrorist financing, and the proliferation of weapons of mass destruction.

2.5 Appointment to the position of responsible employee for internal control is not allowed for the following individuals:

2.5.1 Those who have demonstrated improper management of the entrusted unit in their activities and personal behavior.

2.5.2 Participants or suspects of involvement in terrorist activities or the proliferation of weapons of mass destruction.

2.5.3 Have unspent convictions or pending charges for economic crimes, money laundering, terrorist financing, proliferation financing, organized crime, illegal drug trafficking, corruption, cybercrime, or any related offenses.

LLC 'COINPAY' will conduct thorough background checks to ensure compliance with these requirements

2.6 The responsible employee of the entity engaged in cryptocurrency turnover is appointed from among the managerial staff of LLC 'COINPAY' by the order of the Compliance Officer.

2.7 LLC 'COINPAY' complies with the legal requirement to submit information about its appointed responsible employee to the National Agency for Prospective Projects (NAPP) annually by January 10th, through postal mail or electronic means. In the event of a change in the responsible employee, LLC 'COINPAY' is obligated to notify the NAPP of the newly appointed

individual no later than the next working day after their appointment. The company ensures timely and accurate reporting and maintains records of all such communications.

2.8 The responsible employee performs the following functions:

2.8.1 Takes necessary measures as provided by the legislation of the Republic of Uzbekistan and internal documents of LLC "COINPAY" to prevent the use of services by individuals engaged in activities in the field of cryptocurrency turnover for the purpose of money laundering, financing terrorism, and proliferation of weapons of mass destruction.

2.8.2 Ensures compliance by individuals engaged in activities in the field of cryptocurrency turnover with the requirements of legislation on combating money laundering, financing terrorism, and proliferation of weapons of mass destruction, as well as the legislation of the Republic of Uzbekistan and internal documents of LLC "COINPAY."

2.8.3 Informs the organization's management about violations of legislation related to money laundering, terrorism financing, and proliferation of weapons of mass destruction.

2.8.4 Proposes measures to the organization's management to eliminate identified deficiencies and violations in compliance with the requirements of the legislation of the Republic of Uzbekistan and internal documents of LLC "COINPAY."

2.8.5 Ensures timely transmission of messages to the specially authorized state body about suspicious operations, attempts to commit them, as well as the execution of requests from the specially authorized state body to provide additional information and orders to suspend operations with money or other property of clients.

2.8.6 Coordinates with officials from the National Agency for Prospective Projects (NAPP) and the specially authorized state body to organize internal control measures and to prevent and address violations of AML/CFT regulations.

2.8.7 Disseminates the List among the employees of LLC "COINPAY."

2.8.8 The responsible employee for internal control reports directly to the Compliance Officer of LLC 'COINPAY' and operates independently from other departments or structural units to ensure impartiality and effectiveness in performing AML/CFT duties. The responsible employee is granted sufficient authority, resources, and access to all relevant information necessary to fulfill their responsibilities.

III. IDENTIFICATION AND VERIFICATION OF CLIENTS

3.1 LLC "COINPAY" has established, documented, and maintains a written **Customer Identification Program (CIP)**. For each client transaction, LLC "COINPAY" will:

3.1.1 Collect specific minimum information to identify each client.

3.1.2 Use risk-based measures to verify the identity of each client.

3.1.3 Record client identification information, as well as verification methods and their results.

3.1.4 Screen client identification information against official government-issued lists of known or suspected terrorists and sanctioned individuals or entities, as soon as such lists are made available.

3.1.5 Compare client identification information with global Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) compliance databases, including sanctions lists and adverse media sources

3.2 Client identification is conducted either in the physical presence of the client or through reliable non-face-to-face verification methods that comply with legal requirements, ensuring the authenticity of identification documents and the client's identity.

3.3 Measures for proper client verification include:

3.3.1 Verification of the client's identity and identification; Confirming the client's identity using valid, government-issued identification documents

3.3.2 Identification, verification of identity, and authority of the person acting on behalf of the client, based on relevant documents; Ensuring that representatives are duly authorized and their identities are verified;

3.3.3 Identification of the beneficial owner of the client : determining the ultimate beneficial owner(s) of the client and verifying their identities using appropriate measures;

3.3.4 Examination of the purpose and nature of business relationships or planned transactions : assessing the client's reasons for engaging with LLC 'COINPAY' and the expected activity

3.3.5 Continuously monitoring client activities to ensure they are consistent with the company's knowledge of the client, their business, and risk profile, including, when necessary, the source of funds.

3.4 LLC 'COINPAY' is obliged to take the following measures in relation to **Politically Exposed Persons (PEPs):**

3.4.1 Use risk management procedures to determine whether a client or beneficial owner is a PEP, their family member, or a close associate, and verify the current status of the PEP, as they may no longer hold a PEP position;

3.4.2 If a client or beneficial owner is identified as a current PEP, their family member, or close associate, LLC 'COINPAY' will not establish or continue a business relationship with such individuals in compliance with regulatory requirements and partner constraints;

3.4.3 For clients or beneficial owners who were previously PEPs but are no longer classified as such, LLC 'COINPAY' will verify and document the change in status before considering the establishment or continuation of a business relationship.

3.4.4 Maintain accurate records of all findings related to the PEP status of clients and conduct regular reviews to ensure that the information remains up-to-date and that former PEPs are appropriately classified.

3.4.5 For clients or beneficial owners who were previously PEPs but are no longer classified as such, LLC 'COINPAY' will apply enhanced due diligence measures to verify the status and take reasonable steps to establish the source of wealth and source of funds involved in the business relationship or transaction;

3.4.6 Obtain LLC 'COINPAY' senior management approval before establishing or continuing business relationships for clients or beneficial owners who were previously PEPs;

3.4.7 Conduct enhanced ongoing monitoring of the business relationship, including scrutiny of transactions, to identify any unusual or suspicious activity;

3.5 When a client or a transaction is classified as high-risk, LLC 'COINPAY' applies the following **enhanced due diligence (EDD)** measures

3.5.1 Collecting and verifying additional information on the client, including identification data, occupation, and financial status, from reliable independent sources such as public records and reputable databases;

3.5.2 Obtaining detailed information from the client regarding the source of funds and source of wealth involved in transactions;

3.5.3 Gaining a comprehensive understanding of the purpose and intended nature of the business relationship and transactions;

3.5.4 Increasing the frequency and intensity of monitoring transactions and activities to detect suspicious or unusual patterns.

3.5.5 Requiring senior management approval to establish or continue the business relationship.

3.6 In the absence of the possibility of applying enhanced measures for proper verification of the client, LLC "COINPAY" sends a message about this to a specially authorized state body and refuses to enter into business relations with such a client or from conducting transactions of such a client.

3.7 All identification documents or data used to verify the client and other participants in a transaction must be valid and up-to-date at the time of establishing the business relationship or conducting the transaction. LLC 'COINPAY' must ensure that expired or invalid documents are not accepted for verification purposes."

3.8 If LLC 'COINPAY' is unable to apply the required enhanced due diligence measures to properly verify a high-risk client, the company must:

3.8.1 Refrain from establishing or continuing the business relationship or conducting transactions with the client.

3.8.2 Consider filing a Suspicious Transaction Report (STR) with the specially authorized state body, in accordance with legal obligations.

3.8.3 Document the reasons for the inability to complete enhanced verification measures.

3.9 LLC "COINPAY" has the right to refuse to perform an operation to clients in the case of:

3.9.1 Inability to apply required customer due diligence (CDD) measures due to insufficient or unverifiable information.

3.9.2 Failure to complete client identification or obtain necessary data during the CDD process, indicating that establishing a business relationship would be inadvisable.

3.9.3 Submission of false, misleading, or fraudulent documents, or failure to provide documents required by law or company policy.

3.10 In the event that LLC 'COINPAY' refuses to conduct a transaction or establish a business relationship with a client under the circumstances outlined above, the responsible officer must promptly report the refusal and the underlying reasons to the specially authorized state body, in compliance with legal reporting obligations.

3.11 Required Client Information

Under LLC 'COMPANY's Customer Identification Program (CIP), the following information and supporting documents are required for individual clients:

Individual Accounts

For an individual Client, the following information together with supporting documents will be required:

- Full legal name: As it appears on official identification documents.
- Date of birth: Verified from official documents
- Nationality: As stated on identification documents.
- Residential address**:** Current residential address, including country or area of residence
- Contact information**:** Valid phone number and email address

Supporting documents (individuals):

- Government-issued identification document**:** A clear, legible copy of at least one valid, government-issued photo identification document, such as a national identity card, passport, or driver's license.
- Selfie with identification document: A recent digital photograph (selfie) of the client holding the identification document, clearly showing both the client's face and the document details.
- Proof of residential address: A certified copy or original document showing the client's current residential address, such as a utility bill, bank statement, or government-issued document dated within the last three months.
- Additional documents as required: Any additional documents deemed necessary based on the client's risk profile, such as proof of source of funds or wealth.

Corporate Accounts

For a corporate Client, the following information together with supporting documents will be required:

- Full legal name (should be same as shown in the uploaded incorporation documents)
- Type of business of the applicant (entity)
- Registered address and operation address
- Official website, if applicable
- Government-issued business registration/tax number
- At least one contact person, including name, position, phone number/email address
- Legal structure and information on the applicant’s Ultimate Beneficial

Owner Supporting documents (corporate entities):

- Certified corporate formation document, such as Certificate of Incorporation, Articles of Organization, Memorandum and Articles, etc.
- Certified copy of the register of shareholders
- Certified copy of the register of directors and officers
- Statement signed by at least one director describing the general nature of its business
- Authorized signatory list with specimen signatures of the authorized signatories
- Declaration of Directorship
- Declaration of Beneficial Ownership
- The same required supporting documents for individual accounts for each of the following:
  *Each owner that has 25% or greater ownership, or enough voting power to constitute principal control over such company
  *At least two directors for a board with two or more directors
  *Each and every operating person
- Copy of recent utility bill or bank account statement, which must be addressed to the legal name as provided by the applicant, and its office address

Supporting documents (partnerships):

- Certified copy of the Limited Partnership Agreement or other constitutive document for the entity
- Authorized signatory list with specimen signatures of the authorized signatories
- Certified copy of the register of partners, both limited and general;

Supporting documents (trusts):

- Certified copy of the trust deed showing the trust's names, dates and places of creation
- The names, addresses, nationalities, occupations and dates of birth of all the beneficiaries
- Certified copy of its certificate of registration/license (if any)
- The general nature of the trust (such as family trust, pension trust, charitable trust, etc.)
- Authorized signatory list with specimen signatures of the authorized signatories
- Verification documents and information as set out in this Compliance Manual on the trustee(s) and settlor(s) of the trust as if they were each a client of the Company

For corporate accounts, the Company will also require verification of the entity's current and valid existence in its place of incorporation from the Registry of the jurisdiction of formation. This could be by means of (depending on the jurisdiction): a certificate of good standing; or receipt of payment of license or registration fee (not more than 6 weeks old) issued by the Registry of the jurisdiction of formation.

Method of certification of documentation

- The person certifying must be an independent respected professional that is subject to the professional rules of conduct or statutory compliance measures which carry penalty for breach, for example, a lawyer, notary, bank manager, external accountant, officer of a publicly-listed corporation or registered and licensed dCOINPAYr or dentist.
- The certifier must state his full name, address, telephone number and qualifications under his/her signature.

The requirements for the supporting documents as set out above are general requirements and the Company may deviate from these requirements at the discretion of the Company;

3.12 General Client Due Diligence

It is essential to the Compliance Program that the Company obtain sufficient information about each Client to allow it to evaluate the risk presented by that Client in compliance with applicable laws and regulations. Upon receiving a client's account verification request, LLC 'COINPAY' may perform additional client-level due diligence beyond the scope of its Customer Identification Program (CIP), as deemed necessary based on the client's risk profile.

By adopting a risk-based approach, LLC 'COINPAY' will take appropriate steps to obtain sufficient information to comply with its customer due diligence (CDD) procedures, ensuring that the level of due diligence is commensurate with the client's risk level.

<u>Additional Due Diligence Procedures</u>

LLC 'COINPAY' will ensure that client information remains accurate and up-to-date by performing the following procedures:

- Readability and Legibility: Uploaded identification documents must be clear, legible, and of high quality, with all information fully visible.
- Completeness of Document: Uploaded documents must not have any missing, cropped, or cut-off edges; all edges of the document must be visible to ensure the document is whole and unaltered.

Personal information checking criteria:

- Document Type: The identification document type specified by the client must match the uploaded document provided;
- Name verification: the name on the uploaded identification document should be consistent with the register information
- Identification Number: The identification number on the uploaded document must match the number provided by the client during registration
- Nationality & Residency:
  *the nationality on the uploaded identification document should be consistent with the register information
  *Nationals and residents of the People's Republic of China and the United States of America will ordinarily not be accepted (unless otherwise provided by the Client);
  *Nationals or residents of countries subject to United Nations sanctions or identified by the Financial Action Task Force (FATF) as high-risk or monitored jurisdictions will ordinarily not be accepted, unless adequate measures can mitigate the risks
  * Note**:** LLC 'COINPAY' reserves the right to update the list of restricted jurisdictions in compliance with legal and regulatory changes.
- Date of birth: the Date of Birth on the uploaded identification document should be consistent with the register information
- Document Expiration Date**:** The identification document must be valid and not expired at the time of verification. Documents close to expiration may require renewal prior to acceptance.

Client digital photograph checking criteria:

- Facial Recognition: The person in the digital photograph (selfie) must be the same individual as the holder of the identification document provided. The photograph must clearly show the client's face and the identification document, ensuring all features and details are visible for verification purposes.

(a) General Due Diligence Standards for Corporate Accounts

When the client is a corporate entity or organization, LLC 'COINPAY' will assess the money laundering and terrorist financing risk by considering relevant risk factors. The company may apply all or a subset of these factors based on the entity's nature and complexity.

Relevant risk factors include, but are not limited to:

- Nature of Business and Markets Served: Industry sector, products and services offered, geographical areas of operation, and target markets.
- Type, Purpose, and Anticipated Account Activity: Legal form, reason for opening the account, and expected transaction volume and types.
- Ownership and Control Structure: Complexity of ownership, identification of beneficial owners, and control mechanisms.
- AML/CFT Compliance Record: Information about the entity's compliance history, including any negative media or regulatory actions.
- Regulatory Status and Licensing: Whether the entity is regulated for AML/CFT compliance and holds necessary licenses.

LLC 'COINPAY' will apply its risk-based due diligence procedures and controls to each corporate client's account, ensuring due diligence is appropriate to the assessed risk.

If LLC 'COINPAY' cannot perform appropriate due diligence on a corporate client, the company will:

- Refuse to approve the verification request and refrain from establishing a business relationship or conducting transactions.
- Consider filing a Suspicious Transaction Report (STR) with the specially authorized state body, as required by law.
- Document the reasons for the inability to complete due diligence and the actions taken.

LLC 'COINPAY' will ensure all AML/CFT requirements are satisfied and remain compliant with applicable laws and regulations.

3.13 Clients Who Refuse to Provide Information

If a potential or existing Customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the Company will not verify such potential Client's application request and will make necessary documentation memorializing such decision.

3.14 Non-Face-to-Face Clients

For clients who are not physically present for identification purposes, LLC 'COINPAY' will implement robust non-face-to-face verification procedures, which may include:

3.14.1 Electronic verification through reliable databases or credit reference agencies.

3.14.2. Use of secure digital identification technologies compliant with regulatory standards.

3.14.3 Additional verification measures to mitigate impersonation risk, such as biometric verification or requiring certified copies of documents.

3.15 Verifying Information

Based on the risk, and to the extent reasonable and practicable, LLC 'COINPAY' will ensure that it has a reasonable belief that it knows the true identity of the Clients by using risk-based procedures to verify and document the accuracy of the information it obtains about the Clients. LLC 'COINPAY' will analyze the information received to determine whether or not the information is sufficient to form a reasonable belief that LLC 'COINPAY' knows the true identity of the Client.

LLC 'COINPAY' will verify client identity using documentary means, non-documentary means, or a combination of both, as appropriate. The company will use documentary evidence to verify client identity when suitable documents are available. Given the risks of identity fraud, LLC 'COINPAY' will supplement documentary verification with non-documentary methods whenever necessary. Non-documentary methods may also be employed if there is uncertainty about the client's true identity. In verifying information, the company will consider whether the identifying information received—such as the client's name, address, date of birth, and identification number—allows it to form a reasonable belief that it knows the true identity of the client.

LLC 'COINPAY' may rely on valid government-issued identification documents, such as passports, national ID cards, or driver's licenses, to verify a client's identity.

In addition to documentary methods, **LLC 'COINPAY'** will use non-documentary methods to verify identity, including:

- Obtaining a recent digital photograph (selfie) of the client holding their identification document (ID card or passport), clearly showing the client's face and the document details.
- Utilizing biometric verification techniques where applicable.
- Verifying the client's information against reliable databases, such as credit bureaus or governmental registries

LLC 'COINPAY' will verify the client's information promptly upon receiving an account verification request. If the company discovers suspicious information indicating potential money laundering, terrorist financing, or other suspicious activities, it will, after internal consultation with the Compliance Officer, promptly file a Suspicious Transaction Report (STR) with the specially authorized state body, in accordance with the laws of the Republic of Uzbekistan. The company will ensure compliance with legal obligations while maintaining confidentiality and avoiding tipping off the client.

LLC 'COINPAY' recognizes that the risk of not knowing a client's true identity may be heightened for certain types of clients, such as corporations, partnerships, or trusts that are established in or conduct significant business in jurisdictions identified as high-risk or non-cooperative by international bodies like the Financial Action Task Force (FATF) or sanctioned by the United Nations. The company will identify clients that pose a higher risk of improper identification and will implement enhanced due diligence measures to obtain sufficient information about the identity of individuals associated with the client when standard documentary methods are insufficient. LLC 'COINPAY' will identify clients who have not completed the required identification and verification procedures, including former politically exposed persons (PEPs) and

former government officials. The company will ensure compliance with all regulatory requirements by not establishing or continuing business relationships with such clients until proper due diligence is completed.

3.16 Lack of Verification

If the Company cannot form a reasonable belief that it knows the true identity of a Client, the Company will not verify the application request. All personal data collected during this process will be handled in accordance with data protection laws and LLC 'COINPAY's internal policies to ensure confidentiality and security.

3.17 Recordkeeping

LLC 'COINPAY' will document each client verification process, including all identifying information provided by the client, the methods used for verification, the results obtained, and the resolution of any discrepancies identified during the verification process. LLC 'COINPAY' will maintain records of all client identification and verification documents, as well as transaction records, for a minimum of five (5) years from the date of termination of the business relationship or completion of the transaction, in compliance with the laws of the Republic of Uzbekistan, regardless of whether the client requests storage of the documents. LLC 'COINPAY' will maintain records containing descriptions of all documents relied upon to verify a client's identity, including the type of document, issuing authority, date of issue and expiry, and any identification numbers contained in the document, as part of its standard recordkeeping practices. For non-documentary verification methods, LLC 'COINPAY' will retain detailed records describing the methods used, the data sources consulted, the steps taken to verify the client's identity, and the results of those measures. LLC 'COINPAY' will maintain records documenting the resolution of any substantive discrepancies identified during the verification process, including the nature of the discrepancy, actions taken to resolve it, and the final outcome. LLC 'COINPAY' will ensure that all records are stored securely and protected against unauthorized access, alteration, or destruction, in compliance with data protection laws and company policies. Confidentiality of client information will be maintained at all times. All records will be made readily available to competent authorities and auditors upon legitimate request, in accordance with applicable laws and regulations.

3.18 Comparison with Government-Provided Lists of Terrorists and global AML compliance data

LLC 'COINPAY' will proactively obtain and regularly update the official lists of known or suspected terrorists, terrorist organizations, and sanctioned individuals or entities issued by the government of the Republic of Uzbekistan and relevant international bodies such as the United Nations Security Council. Prior to opening an account or establishing a business relationship, and on an ongoing basis thereafter, the company will screen clients against these lists to determine whether a client or beneficial owner appears on any such list. LLC 'COINPAY' will also screen clients against global Anti-Money Laundering (AML) compliance databases, which may include international sanctions lists, politically exposed persons (PEPs) lists, adverse media databases, and other relevant sources to identify potential risks related to money laundering, terrorist financing, or other financial crimes.

3.19 AML Recordceeping

<u>Responsibility for Required AML Records</u>

The Compliance Officer, or their designated representative, is responsible for ensuring that all Anti-Money Laundering (AML) records are accurately maintained, securely stored, and that all required reports are filed timely and in compliance with the laws of the Republic of Uzbekistan.

LLC 'COINPAY' will maintain all AML records, including customer identification documents, transaction records, and reports filed with regulatory authorities, for a minimum of five (5) years from the date of the termination of the business relationship or the completion of the transaction, in accordance with the laws of the Republic of Uzbekistan.

<u>Document Maintenance and Confidentiality</u>

LLC 'COINPAY' will ensure that all AML records are securely stored with access restricted to authorized personnel only. The company will maintain the confidentiality of all AML records and will not disclose their contents to anyone outside of appropriate law enforcement or regulatory agencies, except as required by law or with the client's explicit consent where permissible.

3.20 AML Training Programs

The Company will develop ongoing employee training under the leadership of the AML Officer and senior management. The Company's training will occur on at least an annual basis. It will be based on the Company's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law. We will let NAPP know when there are changes.

The Company's training will include, at a minimum:

(1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties;

(2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis);

(3) what employees' roles are in the company's compliance efforts and how to perform them;

(4) the Company's record retention policy;

(5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with this AML & Risk Management Policy;

(6) the blockchain technology and common crypto money laundering techniques;

(7) using of Elliptic for transaction monitoring; and

(8) advanced training for the AML team on blockchain forensics and investigation techniques;

The Company will maintain necessary records to show the persons trained, the dates of training and the subject matter of their training and will review its operations to see if certain employees, such as those in compliance and data security, require specialized additional training. The Company's written procedures will be updated to reflect any such changes.

3.21 Unofficial crypto-asset market

Clients engaged in illegal cryptocurrency mining activities, particularly those who mine crypto assets without proper authorization or licenses and subsequently exchange these crypto assets for fiat currency or transfer them abroad.

Clients involved in illegal exchange activities, including:

- Individuals who unlawfully exchange crypto assets for fiat currency or transfer them abroad as part of shadow settlements.
- Persons known as 'changers' who conduct unauthorized exchange of crypto assets for fiat money.
- Individuals organizing or participating in fraudulent 'investment' schemes, such as financial pyramids (Ponzi schemes), utilizing crypto assets.
- Clients using crypto assets for mutual settlements within the 'shadow banking system'.
- Persons trading in prohibited goods (e.g., narcotic or psychotropic substances) using crypto assets.
- Individuals employing unconventional methods of transferring funds, such as 'Hawala', using crypto assets.

Policy on Unofficial Crypto-Asset Market Activities and prohibited industries;

LLC 'COINPAY' strictly prohibits engaging in or facilitating any of the following activities:

- Unauthorized cryptocurrency mining operations.
- Illegal exchange of crypto assets for fiat currency without proper licensing.
- Participation in shadow settlements involving the transfer of crypto assets abroad.
- Involvement in fraudulent investment schemes, including Ponzi or pyramid schemes, using crypto assets.
- Utilizing crypto assets for settlements within unregulated or 'shadow' banking systems.
- Trading in prohibited goods or services, such as narcotics or illegal substances, using crypto assets.
- Employing informal or unregulated methods of fund transfer, such as 'Hawala', using crypto assets.

- Engaging with or providing services to entities involved in prohibited industries, including but not limited to:
    - Arms Trade: Entities engaged in the manufacturing, distribution, or sale of weapons, ammunition, or other military equipment.
    - Defense Industry: Entities involved in the production or provision of defense-related products or services.
    - Mining and Testing Laboratories: Entities operating in mining activities or testing laboratories without proper licensing or regulatory compliance.

Compliance Measures:

- Due Diligence: Enhanced due diligence will be conducted on clients to identify any involvement in the aforementioned activities.
- Transaction Monitoring: Ongoing monitoring of transactions to detect suspicious activities related to the unofficial crypto-asset market.
- Reporting Obligations: Any identified suspicious activities will be promptly reported to the specially authorized state body in accordance with legal requirements.
- Refusal of Service: LLC 'COINPAY' reserves the right to refuse or terminate services to clients involved in illegal activities related to crypto assets.
- Employee Training: Staff will receive regular training on identifying and handling activities associated with the unofficial crypto-asset market

3.22 Sanctions.

3.22.1 LLC 'COINPAY' utilizes relevant sanctions lists for compliance purposes, including those issued by the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury and other international sanctions lists. There is NAAP (National Agency for Advanced Projects) in Uzbekistan that has constantly up-to-date internal list of sanctioned persons that is also used as an informational resource with actual data.

3.22.2 Representatives of LLC 'COINPAY' shall pay special attention to all clients (existing and new), their activities, and any indications that a client may be subject to international sanctions. Screening for potential sanctions exposure shall be conducted by representatives as part of the Customer Due Diligence (CDD) measures applied to clients in accordance with this Policy.

3.22.3 If representatives suspect or become aware that a client is subject to international sanctions, they shall immediately notify the Compliance Officer. In case of doubt, and if deemed appropriate by the Compliance Officer, the representative may request additional information from the client to determine whether the client is indeed subject to international sanctions.

3.22.4 The Compliance Officer is responsible for overseeing the implementation of international sanctions compliance within LLC 'COINPAY'.

3.22.5 The Compliance Officer shall:

- Regularly monitor international sanctions lists and promptly take necessary measures in response to any new sanctions or changes affecting clients or potential clients;
- Terminate or adjust the application of sanctions measures when sanctions are lifted or amended.
- Maintain updated records of sanctioned individuals and entities, providing this information to representatives effectively.
- Provide training to the Representatives that allows them to establish independently the subjects of International Sanctions;
- Assist the Representatives if they have suspicion or knowledge that a Client is a subject of International Sanctions;
- Supervise the application of the Rules regarding the implementation of International Sanctions by the Representatives;
- Regularly review and update this Policy to ensure compliance with legal requirements.

- Keep a record of the performed checks, notifications and the applied measures regarding the detected subjects of International Sanctions.

3.22.6 When conducting checks to determine whether clients are subjects of international sanctions, the following information shall be recorded and retained for a minimum of five (5) years:

- Date and time of the inspection.
- Name of the person who conducted the inspection.
- Results of the inspection, including any findings.
- Measures taken in response to the inspection results.

3.22.7 If, during a check, it is determined that a client or former client is subject to international sanctions, the Compliance Officer shall promptly notify the representatives who have interacted with the client. The notification shall be provided in a form that can be reproduced in writing, such as email or formal memorandum.

3.22.8 When conducting sanctions checks on clients, representatives must be mindful of potential discrepancies or variations in personal information, such as different spellings or transliterations of names, use of aliases, or inconsistencies in identification documents. Careful attention should be paid to ensure accurate identification despite such variations.

3.23 Refund Policy

LLC 'COINPAY' is committed to ensuring client satisfaction with our products and services. We handle every refund request with reasonable care, skill, and diligence, in accordance with this Refund Policy and applicable laws and regulations.

3.23.1 Scope of Refund Policy

- This Refund Policy applies exclusively to:
  - Service Fees: Fees paid by the Client to LLC 'COINPAY' for services rendered.
- This Refund Policy does not apply to:
  - Virtual Currency Transactions: Transactions involving the purchase, sale, exchange, or transfer of virtual currencies, as these are irreversible due to the nature of blockchain technology.

3.23.2 Irreversibility of Virtual Currency Transactions

Clients acknowledge and accept that:

- Finality of Transactions: All transactions involving virtual currencies are final and cannot be reversed once confirmed on the blockchain network.
- No Refunds on Virtual Currencies: LLC 'COINPAY' cannot reverse, cancel, or refund any virtual currency transactions after they have been executed.

3.23.3 Refund Eligibility

Clients may be eligible for a refund of service fees under the following conditions:

- Overpayment: If the Client has overpaid fees due to a processing error.
- Service Non-Delivery: If LLC 'COINPAY' did not deliver the agreed-upon services.
- Service Error: If there was an error in the service provided that is attributable to LLC 'COINPAY'.

3.23.4 Refund Request Process

To request a refund of service fees:

- Submission: Clients must submit a refund request within [insert time frame, e.g., 14 days] of the transaction date.
- Contact Information: Refund requests should be sent to [insert contact email or form link].
- Required Information: The request must include the Client's full name, account details, transaction ID, date of transaction, amount, and a detailed explanation of the reason for the refund.

3.23.5 Refund Assessment and Processing

- Review Period: LLC 'COINPAY' will review the refund request within [insert time frame, e.g., 5 business days] of receipt.
- Decision Notification: The Client will be notified of the decision via email or through their account portal.
- Refund Method: Approved refunds will be credited back to the original payment method used by the Client.
- Refund Limits: The refund amount will not exceed the original service fee paid by the Client for the specific transaction in question.

3.23.6 Exceptions and Exclusions

Refunds will not be granted in the following circumstances:

- Policy Violations: If the Client has violated any terms of the User Agreement, Terms of Service, or any applicable laws and regulations.
- Third-Party Services: Fees or charges imposed by third-party service providers are not refundable.
- Market Fluctuations: Losses due to changes in the market value of virtual currencies are not eligible for refunds.

3.23.7 Amendments to the Refund Policy

- Policy Changes: LLC 'COINPAY' reserves the right to modify or update this Refund Policy at any time to reflect changes in our practices or for other operational, legal, or regulatory reasons.
- Notification: Clients will be notified of significant changes to this policy through the website or via email.

3.23.8 Legal Compliance

- Applicable Laws: This Refund Policy is governed by the laws of the Republic of Uzbekistan.
- Dispute Resolution: Any disputes arising from this policy shall be resolved in accordance with the dispute resolution procedures outlined in the Terms of Service.

3.23.9 Client Acknowledgment

By using LLC 'COINPAY' services, the Client acknowledges that they have read, understood, and agreed to this Refund Policy.

3.24 Chargeback Policy

3.24.1 Rights of the Client

This Chargeback Policy does not limit or affect any rights and/or claims the Client may have against their bank or financial institution under applicable laws and regulations.

3.24.2 Chargeback Procedure

In the event that a Client initiates a chargeback request with their bank or financial institution regarding a transaction processed through LLC 'COINPAY', the following steps will be taken:

a. Investigation: LLC 'COINPAY' will conduct a thorough investigation of the chargeback request within a reasonable timeframe to determine the validity of the claim.

b. Communication with Financial Institution: We will provide all necessary information and documentation to the Client's bank or financial institution to assist in resolving the chargeback request, including confirmation of whether the transaction in question has been canceled or completed.

3.24.3 Encouragement to Resolve Issues Directly

We strongly encourage Clients to contact LLC 'COINPAY' directly to resolve any refund or transaction issues before initiating a chargeback request with their bank or financial institution. Our customer support team is available to assist in addressing any concerns or disputes promptly.

3.24.4 Suspension of Services During Investigation

LLC 'COINPAY' reserves the right to temporarily suspend the Client's access to our Services during the chargeback investigation process. This measure is taken to protect all parties involved and to prevent potential misuse of our Services.

3.24.5 Consequences of Unresolved Chargebacks

a. Account Review: If a chargeback is not resolved in favor of LLC 'COINPAY', we may review the Client's account for potential violations of our Terms of Service or policies.

b. Termination of Services: Repeated or unwarranted chargeback requests may result in termination of the Client's account and access to our Services, in accordance with our Terms of Service.

3.24.6 Legal Compliance

a. Applicable Laws: This Chargeback Policy is governed by the laws of the Republic of Uzbekistan.

b. Dispute Resolution: Any disputes arising from this policy shall be resolved in accordance with the dispute resolution procedures outlined in our Terms of Service.

3.24.7 Client Acknowledgment

By using LLC 'COINPAY' Services, the Client acknowledges that they have read, understood, and agreed to this Chargeback Policy.

IV. IDENTIFICATION AND ASSESSMENT OF THE RISK LEVEL

4.1 LLC 'COINPAY implements a comprehensive risk management framework to effectively **identify**, **assess**, **monitor**, **manage**, **document**, and **mitigate** risks associated with money laundering, terrorist financing, and proliferation financing. The risk assessment shall be conducted by the Compliance Officer or a designated responsible employee, utilizing the Know Your Customer (KYC) software system and dashboard. This assessment is based on:

- Information provided by the client, including personal data, business activities, and transaction purposes.
- Nature and purpose of the client's activities and transactions, considering the expected use of services.
- Criteria established by the laws and regulations of the Republic of Uzbekistan, ensuring legal compliance.
- Internal policies and procedures of LLC 'COINPAY', aligning with the company's risk appetite and control measures.

- Results of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) processes, identifying the client's risk profile.
- Identified risk factors, such as:
    - Customer Risk: Type of customer, occupation, reputation, and whether they are a former Politically Exposed Person (PEP).
    - Geographic Risk: Countries or regions where the client operates, especially high-risk jurisdictions.
    - Product/Service Risk: Complexity and transparency of products or services used.
    - Transaction Risk: Unusual transaction patterns, large volumes, or transactions inconsistent with the client's profile.
- Analysis of any other relevant information obtained during client onboarding and ongoing monitoring.

4.2 Adoption of Risk-Based Approach

LLC 'COINPAY' adopts a **risk-based approach (RBA)** to Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) compliance, ensuring that resources are allocated efficiently and measures are proportionate to the identified risks. Higher-risk clients and transactions will receive enhanced scrutiny, while lower-risk cases may be subject to simplify the due diligence process where permitted by law."

4.3 High-Risk Clients:

4.3.1 Persons who are included on official sanctions lists or watchlists issued by competent authorities, or individuals who are directly or indirectly controlled by, or acting on behalf of, such persons, including beneficial owners or controllers of organizations listed on these sanctions lists.

4.3.2 Persons who are permanently residing, located, or registered in jurisdictions identified as having strategic deficiencies in their AML/CFT regimes, including countries subject to sanctions, embargoes, or other restrictive measures by international organizations (e.g., FATF high-risk and other monitored jurisdictions), as well as offshore financial centers known for inadequate transparency.

4.3.3 Clients who are representative offices of foreign companies or non-resident individuals from high-risk jurisdictions, specifically those identified as high-risk or non-cooperative in AML/CFT efforts, or those presenting higher risk due to their location or nature of business.

4.3.4 Persons who hold accounts in offshore jurisdictions known for secrecy laws, lack of transparency, or insufficient AML/CFT measures.

4.3.5 Organizations whose beneficial owners are individuals identified in the high-risk categories above (4.2.1 and (or) 4.2.2), including those on sanctions lists or from high-risk jurisdictions.

4.3.6 Clients who engage in suspicious transactions on a recurring basis, such as conducting more than two suspicious transactions within any three-month period.

4.3.7 People, who were previously included in Politically Exposed Persons (PEPs) lists, including domestic and foreign public officials, their immediate family members, and close associates.

4.3.8 Clients who conduct transactions involving cryptocurrency mixing or tumbling services, or utilize privacy-enhanced cryptocurrencies ('privacy coins') designed to obfuscate transaction trails (to be flagged by Know Your Transaction (KYT) monitoring systems).

4.3.9 Clients who conduct transactions involving sudden large deposits or withdrawals of cryptocurrencies exceeding USD 10,000, which are inconsistent with their known profile or expected activity (to be flagged by KYT monitoring systems).

4.3.10 Clients who engage in transactions involving cryptocurrency addresses linked to darknet marketplaces, illicit activities, or known fraudulent schemes (to be flagged by KYT monitoring systems).

4.3.11 Clients who engage in transactions involving cross-chain transactions and blockchain bridge services, particularly when used to obscure the origin or destination of funds (to be flagged by KYT monitoring systems).

4.3.12 Clients who conduct transactions involving decentralized finance (DeFi) platforms, especially when such platforms are unregulated or have been associated with illicit activities or vulnerabilities (to be flagged by KYT monitoring systems).

4.3.13 Clients who engage in transactions involving non-fungible tokens (NFTs), particularly high-value NFTs or patterns indicative of potential money laundering or fraudulent activities (to be flagged by KYT monitoring systems).

4.4 High-risk jurisdictions

COINPAY LLC should not establish or maintain business relationships with individuals or entities located in, or conducting

transactions involving, countries subject to FATF's call for action (e.g., North Korea and Iran); Apply EDD measures for customers and transactions involving countries under increased monitoring by the FATF ("Grey List") and those subject to international sanctions. This includes obtaining additional information on the customer and beneficial owner, the intended nature of the business relationship, and the source of funds.

4.4.1 High-Risk Jurisdictions Subject to a Call for Action:

- Democratic People's Republic of Korea (DPRK)
- Iran
- Myanmar (Burma)

4.4.2 Jurisdictions Subject to International Sanctions:

- Russia: Subject to comprehensive sanctions by the United States, European Union, United Kingdom, and other countries due to its actions in Ukraine.
- Belarus: Facing sanctions related to human rights abuses and support for Russia's activities in Ukraine.
- Syria: Under sanctions due to ongoing conflict and human rights violations.
- Venezuela: Sanctioned for undermining democratic processes and human rights abuses.
- Cuba: Subject to U.S. sanctions related to human rights and political freedoms.

4.4.3 Jurisdictions Under Increased Monitoring ("Grey List"):

Algeria; Angola; Burkina Faso; Cameroon; Côte d'Ivoire; Croatia; Democratic Republic of the Congo; Haiti; Kenya; Lebanon; Mali; Monaco; Mozambique; Namibia; Nigeria; Philippines; Senegal; South Africa; South Sudan; Syria; Tanzania; Venezuela; Vietnam; Yemen;

Customers and entities from countries under increased monitoring ("Grey List") are classified as a **high-risk**, requiring Enhanced Due Diligence;

4.5 Enhanced Due Diligence Measures for High-Risk Clients

LLC 'COINPAY' shall apply enhanced due diligence (EDD) measures to all clients classified as high-risk, which may include:

- Obtaining additional identification documents or information.
- Verifying the source of funds and wealth.
- Conducting more frequent and thorough ongoing monitoring of transactions.
- Requiring senior management approval to establish or continue the business relationship.
- Implementing stricter transaction limits or controls
- Conducting quarterly reviews for high-risk clients to ensure ongoing compliance and risk management

4.6 Risk Assessment for New Products, Services, and Technologies

LLC 'COINPAY' shall implement measures to prevent the misuse of technological advancements for the purposes of money laundering, terrorist financing, and financing the proliferation of weapons of mass destruction. To achieve this, the company must:

- Identify and Assess Risks: Proactively identify and assess the levels of risk that may arise from:
  The development of new products, services, or business practices, including the adoption of innovative delivery mechanisms.
  The use of new or emerging technologies in both new and existing products and services.

- Conduct Prior Risk Assessments: Ensure that such risk assessments are conducted **prior** to the launch or use of new products, services, business practices, or technologies.
- Implement Risk Mitigation Measures: Develop and implement appropriate policies, procedures, and controls to manage and mitigate identified risks to acceptable levels.
- Monitor and Review: Continuously monitor the effectiveness of these measures and make necessary adjustments in response to changes in the risk environment or regulatory requirements.
- Compliance with Legal and Regulatory Requirements: Ensure all actions are in compliance with the laws of the Republic of Uzbekistan and align with international best practices, including the Financial Action Task Force (FATF) Recommendations.

4.6.1 Collaborating with Regulatory Authorities

Where appropriate, LLC 'COINPAY' shall consult with relevant regulatory authorities regarding the introduction of new products, services, or technologies to:

- Ensure compliance with regulatory expectations.
- Obtain guidance on managing and mitigating AML/CFT risks.
- Contribute to the development of industry best practices.

4.6.2 Technology Controls

Implement robust technological controls to mitigate risks associated with new technologies, including:

- Security measures to protect against cyber threats.
- Systems to monitor and detect suspicious activities in real-time.
- Regular testing and updating of technological systems to address vulnerabilities.

V. CRITERIA AND SIGNS OF SUSPICIOUS TRANSACTIONS

5.1. An operation is considered suspicious if one of the following criteria and signs is present:

5.1.1. The submitted documents related to the transaction raise doubts about their authenticity or reliability.

5.1.2. Information provided about the transaction, including details of any parties involved, does not correspond with information obtained from reliable sources or does not make logical sense.

5.1.3. The transaction lacks an apparent economic or lawful purpose. The transaction is inconsistent with the client's known business activities or profile;

5.1.4. The client unreasonably refuses to provide information necessary for identification and verification processes, including information about the principal if the client is acting on behalf of another person.

5.1.5. The client initiates immediate termination of the business relationship upon being subjected to legal requirements or internal policies, such as KYC, CDD, or transaction monitoring procedures.

5.1.6. It is impossible to complete the identification and verification process of the client.

5.1.7. The results of due diligence indicate that establishing or continuing a business relationship with the client would be inadvisable or pose significant risk.

5.1.8. The client's neglect of more favorable conditions for the provision of services, as well as the client's offer of an unusually high remuneration, obviously different from what is usually paid for the provision of such services;

5.1.9. Crypto assets or funds are transferred outside the Republic of Uzbekistan to individuals or entities permanently residing or registered in offshore jurisdictions known for weak AML/CFT controls or secrecy laws.

5.1.10. A party involved in the transaction is permanently residing, located, or registered in a jurisdiction identified as non-cooperative or high-risk in international AML/CFT efforts, including those under sanctions or subject to FATF public statements.

5.1.11. The client engages in repeated transactions that appear designed to evade legal reporting thresholds or circumvent AML/CFT control procedures.

5.1.12. The client regularly transfers crypto assets of the same amount to the same crypto wallet or multiple wallets, including those held on crypto exchanges, without a clear economic purpose.

5.1.13. The client engages in multiple exchanges of different crypto assets, followed by withdrawals to crypto wallets on other exchanges, platforms, or private wallets, potentially to obscure the transaction trail.

5.1.14. High Volume Transactions in Short Time Frames: The client conducts a large number of high-value crypto asset transactions within a 24-hour period and (or) the client uses newly opened or previously dormant crypto wallets for such activities.

5.1.15. The client suddenly transfers crypto assets to individuals or entities involved in crypto asset activities in countries where the client does not have apparent business relationships or legitimate reasons for such transactions.

5.1.16. The client invests in crypto assets and then transfers them to private or anonymous crypto wallets within a short period, potentially to conceal the origin or ownership of the assets.

5.1.17. The client receives crypto assets from wallets known to have been used for illicit activities and (or) the client interacts with wallets associated with individuals who previously owned wallets involved in criminal purposes.

5.1.18. The client deposits large amounts of crypto assets into wallets, which are inconsistent with their normal transaction volume or known financial profile.

5.1.19. The client exchanges crypto assets for fiat currency at significantly higher commissions or unfavorable exchange rates without a reasonable explanation.

5.1.20. A newly issued crypto asset experiences a rapid increase in value and is traded exclusively on a single crypto exchange or platform, which may indicate market manipulation or fraudulent activities.

5.1.21. There are signs that the client is involved in or benefiting from manipulation of crypto asset prices, such as coordinated trading, pump and dump schemes, or dissemination of misleading information.

5.1.22. The client exchanges newly issued crypto assets for well-known, long-standing crypto assets and then immediately withdraws them to multiple wallets or converts them into fiat currency.

5.1.23. Lack of Transparency in New Crypto Asset Offering: the newly issued crypto asset lacks a 'White Paper' or equivalent disclosure document. The White Paper contains false, misleading, or inconsistent information, such as unfounded claims of backing by governments or reputable companies. Funds raised are directed towards suspicious or unverified investment projects.

5.1.24. The client consistently uses services designed to conceal their IP address or identity, such as VPNs, TOR networks, or other anonymizing tools, without a legitimate reason.

5.1.25. There are inconsistencies between the client's actual domain or that of their transaction counterparty and the domain corresponding to the country of their registration or operation.

5.1.26. The client opens a large number of crypto wallets from a single IP address, which may indicate attempts to circumvent transaction limits or obscure transaction origins;

5.1.27. The client frequently changes their identification information such as email addresses, IP addresses, domains, or ownership details of crypto wallets without a legitimate reason;

5.1.28. The client demonstrates a lack of knowledge or understanding of crypto assets and related transactions, inconsistent with the level of activity or investment they are undertaking.

5.1.29. The client's crypto assets originate from online gambling platforms or services that facilitate risk-based games, which may be associated with higher money laundering risks.

5.1.30. There is any suspicion that the funds or assets involved in the transaction have a criminal origin, or are intended for use in money laundering, terrorist financing, or financing the proliferation of weapons of mass destruction.

5.1.31. The client engages in repeated transactions involving crypto addresses associated with mixing or tumbling services, or utilizes privacy coins designed to obscure transaction details.

5.1.32. The client conducts repeated transactions involving crypto addresses associated with darknet marketplaces, illicit activities, or known fraudulent schemes.

5.1.33. The client repeatedly engages in transactions involving addresses linked to cross-chain transactions and blockchain bridge services, particularly where such services may be used to obscure the origin or destination of funds.

5.1.34. The client repeatedly conducts transactions involving addresses associated with decentralized finance (DeFi) platforms or non-fungible token (NFT) platforms, particularly when these platforms are unregulated or have been linked to illicit activities.

5.1.35. Unusual geographic patterns: transactions are conducted with countries or regions that are known for high levels of corruption, criminal activity, or are subject to sanctions, without a clear business rationale.

5.1.36. Transactions that are significantly larger or more frequent than expected based on the client's known income or business activities.

5.1.37. The client frequently uses third parties or intermediaries in transactions without a clear business reason, potentially to conceal the true beneficiary or originator."

5.2. LLC 'COINPAY' reserves the right to establish and implement additional criteria and indicators for identifying suspicious transactions beyond those stipulated by law, to enhance its Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) measures.

5.3. LLC "COINPAY" may implement indicators for the early detection of questionable and suspicious transactions based on methodological recommendations developed by NAPP in coordination with a specially authorized state body and having a recommendatory character.

5.4. LLC 'COINPAY' shall pay special attention to all complex, unusually large transactions, and unusual patterns of transactions that have no apparent economic or lawful purpose. Such transactions shall be thoroughly examined, and if deemed suspicious, they must be promptly reported to the specially authorized state body in accordance with legal requirements.

5.5. Employees of LLC 'COINPAY', in accordance with their official duties, are responsible for conducting client identification and ongoing monitoring of their transactions. If, during these processes, an employee detects transactions exhibiting signs of suspicious activity, they are obligated to immediately report such transactions to the designated Compliance Officer or the responsible internal control officer.

5.6. The information obtained during the identification and verification process, along with the assigned risk level for the client, forms the basis for monitoring their transactions and activities. This ensures that the level of scrutiny applied is commensurate with the client's risk profile.

5.7. The responsible employee, such as the Compliance Officer, shall conduct subsequent verification of the client's transactions by analyzing historical transaction patterns to identify any suspicious transactions that may not have been detected during ongoing monitoring. If reasonable suspicions arise, the responsible employee must document the findings and make a formal decision to classify the transaction as suspicious.

5.8. The recognition of a transaction as suspicious is determined on a case-by-case basis through a comprehensive analysis using:

5.8.1. The criteria for suspicion established by the laws of the Republic of Uzbekistan.

5.8.2. Internal policies and procedures of LLC 'COINPAY'.

5.8.3. The client's risk profile, including the type of client, purpose and size of transactions.

5.8.4. Other relevant circumstances that may affect the determination of suspicion.

5.9. After identifying a client's transaction as suspicious, the responsible employee (e.g., the Compliance Officer) must take the following actions:

- Strengthen monitoring of the client's activities: enhance the level and frequency of monitoring of the client's transactions and activities to detect any further suspicious behavior promptly.
- Conduct enhanced due diligence : obtain additional information about the client by performing Enhanced Due Diligence, including verifying the client's identity, background, and risk factors more thoroughly.
- Gather detailed information about the source of funds involved in the suspicious or large transactions to assess their legitimacy;
- Utilize blockchain analysis tools to trace the history of incoming and outgoing funds associated with the transaction, identifying any links to illicit activities or high-risk entities;
- Record all relevant information and findings related to the suspicious transaction in a secure and confidential log, ensuring proper documentation for compliance and auditing purposes;
- Immediately report the findings and all pertinent information to the Compliance Officer and the Compliance Officer for further assessment and action
- Ensure that a Suspicious Transaction Report (STR) is prepared and submitted to the specially authorized state body promptly, and no later than one working day from the time the suspicious transaction is detected, in accordance with legal requirements;
- Evaluate the necessity of recommending to senior management or the head of LLC 'COINPAY' the termination of the business relationship with the client, in accordance with applicable laws and contractual agreements;
- Increase the frequency of reviews for the client, conducting quarterly reviews for high-risk clients and maintaining annual reviews for low-risk clients, to ensure ongoing compliance and risk management.

5.10. Submission of Suspicious Transaction Report (STR). The Compliance Officer or designated internal control officer shall prepare and submit a Suspicious Transaction Report (STR) to the specially authorized state body promptly, and no later than

one working day from the time the suspicious transaction is detected, following the procedures prescribed by law.

5.11. LLC 'COINPAY' must promptly provide the specially authorized state body with any additional information that may confirm or dispel suspicions regarding the transaction, ensuring full cooperation with ongoing investigations.

5.12. All actions taken and information obtained during the investigation of a suspicious transaction must be kept confidential. Employees are prohibited from disclosing any details to the client or unauthorized parties, as such disclosure (tipping-off) is prohibited by law.

5.13. Following the identification of a suspicious transaction, the Compliance Officer should review the effectiveness of existing internal controls and procedures, implementing enhancements if necessary to prevent future occurrences

VI. OPERATIONS CARRIED OUT WITH THE PARTICIPATION OF PERSONS INVOLVED OR SUSPECTED OF PARTICIPATING IN TERRORIST ACTIVITIES OR THE DISTRIBUTION OF WEAPONS OF MASS DESTRUCTION

6.1 Obligation to Screen Against Sanctions and Prohibited Lists LLC 'COINPAY' is obligated to verify the identification data of clients, beneficial owners, and any participants involved in transactions against relevant sanctions and prohibited lists, including:

- United Nations Security Council Resolutions lists.
- National sanctions lists issued by the Republic of Uzbekistan.
- Other international lists of designated persons involved in terrorism or proliferation of weapons of mass destruction (WMD).

6.2 If, during client onboarding or transaction processing, employees of LLC 'COINPAY' identify an exact match between the identification data of a client, beneficial owner, or any participant in a transaction and a person listed on the sanctions or prohibited lists, they must immediately:

- Suspend the transaction and/or freeze the related crypto assets without prior notice to the client (to prevent tipping-off).
- Notify the Compliance Officer or the designated internal control officer immediately.
- Refrain from conducting any further transactions with the client until clearance is obtained from the relevant authorities.

6.3 The Compliance Officer or designated internal control officer must:

- Record all relevant identification data of the client, beneficial owner, or participant involved in the transaction, as well as details of the transaction itself, in a secure and confidential log.
- Prepare and submit a report to the specially authorized state body (e.g., the Financial Intelligence Unit of the Republic of Uzbekistan) without delay, following the prescribed legal procedures.
- Ensure all records are maintained in accordance with data protection laws and record-keeping requirements.

6.4 An operation involving crypto assets must be suspended immediately, without prior notice to the client, and the assets must be frozen and reported to the specially authorized state body if any of the following conditions are met:

6.4.1 An exact match of all identification data of the client, beneficial owner, or any participant in the transaction with a person included in the sanctions or prohibited lists.

6.4.2 The client is acting on behalf of or at the direction of a person included in the sanctions lists.

6.4.3 The funds, crypto assets, or other property used in the transaction are wholly or partially owned or controlled by a person included in the sanctions lists.

6.4.4 A legal entity participating in the transaction is owned or controlled, directly or indirectly, by a person included in the sanctions lists.

6.5 When LLC 'COINPAY' suspends a transaction and/or freezes funds or crypto assets associated with a person included in the sanctions lists, the company must:

- Prepare and submit a Suspicious Transaction Report (STR) to the specially authorized state body, such as the Financial Intelligence Unit, immediately and no later than one working day from the time of suspension.
- Include in the report all relevant details, including the identification data of the parties involved, the nature of the transaction, and the amount and type of assets frozen.
- Maintain confidentiality and refrain from disclosing any information about the reporting or freezing action to the client or third parties.

VII. PROVISION OF INFORMATION TO THE SPECIALLY AUTHORIZED STATE BODY

7.1 LLC 'COINPAY' shall ensure that the Compliance Officer or designated internal control officer promptly prepares and submits a Suspicious Transaction Report (STR) to the specially authorized state body, such as the Financial Intelligence Unit (FIU) of the Republic of Uzbekistan, in accordance with legal requirements. The STR must be submitted immediately,

and no later than one working day following the detection of the suspicious transaction.

7.2 All information related to each STR submitted must be accurately recorded in a secure and confidential Special Register maintained by the Compliance Officer or responsible employee. The records should include:

- Details of the suspicious transaction reported.
- Date and time of the report submission.
- Copies of the STR and any supporting documentation.

These records must be stored securely and retained for a minimum of five (5) years in accordance with legal and regulatory requirements.

7.3 For transactions subject to notification to the specially authorized state body in accordance with the legislation of the Republic of Uzbekistan and the internal documents of LLC "COINPAY", they are documented with a record in a special journal:

7.3.1 Type of Transaction and Reason for Execution.

7.3.2 Date and Amount of Transaction.

- The exact date and time the transaction was conducted.
- The total amount involved in the transaction, specifying the currency and any applicable exchange rates

7.3.3 Client Identification Information:

- Full legal name of the client and any aliases.
- Identification document details (e.g., passport number, national ID).
- Residential or business address.
- Contact information (phone number, email address).
- Beneficial owner information, if applicable.

7.4 LLC 'COINPAY' is obligated to promptly provide the specially authorized state body with any additional information that may confirm or refute the suspicion related to a reported transaction. This includes:

- Responding to requests for information from the FIU or other competent authorities.
- Voluntarily providing new information discovered after the initial report that is relevant to the investigation.
- Ensuring all communications are conducted confidentially and securely.

VIII. DOCUMENTATION, STORAGE, AND CONFIDENTIALITY OF INFORMATION

8.1 Information about the client obtained during the proper verification process is indicated in the client questionnaire according to Appendix No. 3 to this Policy.

8.2 Questionnaires are filled out electronically for all clients (except for clients for whom no verification measures are required) using special programs. The register of client questionnaires, conducting dubious and/or suspicious transactions, and clients classified as high-risk is kept in electronic form.

8.3 Electronic versions of completed questionnaires are stored in a database that allows employees of LLC "COINPAY", responsible for client identification, as well as payment agents and subagents, to have real-time access for checking client information.

8.4 As the information provided in the client questionnaire changes, as well as the nature of their financial transactions, LLC "COINPAY", when necessary, reviews the level of risk associated with working with them.

8.5 Information about transactions must be documented in a way that allows details of the transaction to be reconstructed if necessary.

8.6 LLC “COINPAY” retains information about transactions, as well as identification data and materials from proper client verification, account files, business correspondence, and the results of any analysis conducted for periods established by legislation, but not less than five years after the transactions are completed or business relations with clients are terminated.

8.7 LLC “COINPAY” ensures that its employees do not disclose (or use for personal purposes or the interests of third parties) information obtained during the performance of their internal control functions.

8.8 Information obtained as a result of proper client verification must be updated based on significance and risks, and in case of changes in client information, but no less than once a year in cases where LLC “COINPAY” assesses the risk of a client engaging in money laundering, financing terrorism, and financing the proliferation of weapons of mass destruction as high, and in other cases, no less than once every two years.

IX. RESPONSIBILITY OF MANAGERS AND EMPLOYEES OF THE INTERNAL CONTROL SERVICE AND OTHER DEPARTMENTS

9.1 The Director, Senior Management, and all employees of LLC 'COINPAY', including those in the Internal Control Service and other departments, are individually and collectively responsible for:

- Complying with this Policy, the laws of the Republic of Uzbekistan, and all internal documents related to Anti-Money Laundering (AML), Counter Financing of Terrorism (CFT), and Counter Proliferation Financing (CPF).
- Performing their duties with integrity, due diligence, and in accordance with established ethical standards.
- Staying informed about updates or changes to policies, laws, and regulations relevant to their roles.

9.2 Employees who become aware of any violations of laws, regulations, this Policy, or internal procedures—including those related to AML/CFT/CPF—committed by any personnel of LLC 'COINPAY' during operations must:

- Immediately report these incidents in writing to the Director, Compliance Officer, or the designated Internal Control Officer.
- Provide all relevant details and evidence to facilitate a thorough investigation.

9.3 LLC 'COINPAY' ensures that employees who report violations in good faith are:

- Protected from retaliation, discrimination, or any negative consequences resulting from their reports.
- Encouraged to come forward without fear, promoting a culture of transparency and integrity.

Appendix №1
To the AML & risk management policy of LLC «COINPAY»

INFORMATION
required for the identification of individuals

1. Surname, first name, and patronymic (if applicable).
2. Date and place of birth.
3. Citizenship.
4. Place of permanent and/or temporary residence.
5. Passport details or details of the document replacing it: series and number of the document, date of issue, issuing authority.
6. Personal identification number of the individual.
7. Mobile phone number (if available).

Appendix №2
To the AML & risk management policy of LLC «COINPAY»

INFORMATION
for the identification of legal entities, non-legal entities, and individual entrepreneurs

1. Information required for the identification of legal entities and non-legal entities:
a) Full and abbreviated name, if specified in the certificate of state registration;
b) Information about state registration: date, number, name of the registering authority;
c) Tax identification number;
d) Location (postal address);
e) Other data specified in the certificate of state registration;
f) Information about licenses for activities subject to licensing: type of activity, license number, date of issuance, issuing authority, validity period;
g) Data on the identification of individuals authorized to sign or act on behalf of the legal entity;
h) Information about founders (major shareholders, participants) and their shareholding in the authorized capital (capital) of the legal entity;
i) Information about the registered and paid-up charter capital (capital);
j) Information about the management bodies of the legal entity (structure and personnel composition of the management bodies of the legal entity);
k) Phone numbers.

2. Information required for the identification of individual entrepreneurs:
a) Information provided in Appendix 1 to the Rules of Internal Control for Combating Money Laundering and Terrorism Financing in Commercial Banks;

b) Information about state registration: date, number, name of the registering authority;
c) Place of business activity;
d) Other data specified in the certificate of state registration;
e) Information about existing certificates and licenses for activities: type of activity, number, date of issuance, issuing authority, validity period;
f) Phone numbers.

Appendix №3
To the AML & risk management policy of LLC «COINPAY»

INFORMATION
provided in the Client Questionnaire

1. Information obtained during the client identification process, as specified in Appendices No. 1 and 2 to the Internal Control Rules for Combating Money Laundering at LLC "COINPAY".
2. Data on the beneficial owner of the client.
3. Indication of whether the client is a public official (or a family member or close associate of a public official).
4. Risk level information, including rationale for risk assessment.
5. Results of additional measures conducted during client identification.
6. Start date of Client relationship.
7. Date of completion and any changes made to the client questionnaire.
8. Full name, position of the employee responsible for client interaction.
9. Signature of the employee who completed the client questionnaire on paper (with indication of their full name and position) and the full name, position of the employee who completed the client questionnaire in electronic form.
10. Other data