QOINY LLC COMPANY

POLICY ON PREVENTION OF MONEY LAUNDERING AND COMBATING TERRORISM FINANCING

Prishtina

June 2024

Contents

1. Introduction

Money Laundering is the process by which illegally obtained money, crypto-currency or other property is exchanged for "clean" money or other assets with no obvious link to their criminal origins. The term is used for number of illegal activities involving integration of "dirty money" into the financial sector and economy. The aim is to legitimize the possession of such money through circulation of it in financial sector, and this effectively leads to "clean" funds being received in exchange.

Qoiny LLC (hereafter: the company) is committed to to conducting its business with the highest ethical and legal standards, therefore it expects all employees and other persons related to the company, to act accordingly. As such, the company has adopted this Anti-Money Laundering/Combating Finance of Terrorism Policy, which is applicable to shareholders, directors, managers, officers, agents, and employees of the company.

Company's intention is to avoid conducting business with individuals and/or companies who may negatively impact the profile of the company, by increasing the risk of conducting suspicious activities through the company.

2. Purpose of the Policy

The purpose of AML Policy is to set the clear objectives of the company towards prevention of money laundering and terrorism financing activities through its products and services, by establishment of effective mechanisms to create detailed profile of onboarding clients through KYC process and screening against international sanctions lists, and to maintain updated information through clients' due diligence and transaction monitoring processes.

Besides above-mentioned preventive mechanisms, the company is committed to have well trained staff on AML/CFT matters, by providing continuous introductory and refreshment training sessions on detection, managing and reporting of suspicious activities of clients.

3. Scope of Policy

AML Policy is focused to set principles of effective control mechanisms which will serve as prevention suspicious clients and activities, and detection of suspicious transactions of clients. Control mechanisms consist of automized controls which function based on certain scenarios, and staff controls which ensure an effective assessment of each unusual activity that has been detected.

4. Key principles of AML Policy

Key principles of the company which should be complied by all staff, are ranked below:

- Complying with all Anti-Money Laundering Act and Regulations
- Requiring all employees to prevent, detect and report to the AML Officer all potential cases that can be associated with AML Risk.
- Providing AML Officer all necessary information, documents and support at all times.
- Requiring all appropriate employees to attend anti-money laundering training sessions, so all employees are aware of their responsibilities under company's policies and procedures.
- Protecting the firm and all its staff as individuals from the risks associated with the breach of AML Law, regulations and other legislative and regulatory requirements.
- Preserving the good name of the company against the risk of the reputational damage presented by implication in money laundering and terrorist financing activities.

It shall be the policy of this company that:

- Every member of staff shall meet their personal obligations as appropriate to their role and position in the company.
- Neither commercial considerations nor a sense of loyalty to clients shall be permitted to take precedence over the firm's anti-money laundering commitment.
- The company shall carry out a business wide assessment of the risk of money laundering and terrorist financing to which the company is subject and design and implement appropriate controls to mitigate and manage effectively the risks identified.
- The firm shall establish and maintain documented, proportionate policies and procedures, including controls, which outline the positive actions to be taken by staff to prevent money laundering and terrorist financing in the course of their work.

5. Legislative Framework

The company is committed to be fully in compliance with the legislative requirements of Law on AML/CTF of Republic of Kosovo, and with the international standards as orientation point for prevention and management of AML Risk.

Obligations of the company related to Anti-Money Laundering and Combating Terrorism Financing are to:

- Appoint a AML Officer
- Obtain sufficient knowledge to ascertain the true identity of customers in certain circumstances, by applying customer due diligence measures.
- Know the intended nature of business relationships and undertake ongoing monitoring of them (to identify unusual transactions);

- Reporting the suspected activities and transactions of customers to Financial Intelligence Unit of Kosovo within 24 hours of their identification;
- Maintain record keeping procedures (e.g. for evidence of identity obtained, details of transactions undertaken for at least 5 years);

6. Function of AML/CFT

Company shall appoint one staff as responsible person for implementation of AML/CFT requirements (AML Officer). Appointed person shall be responsible for implementation of AML/CFT requirements including client identification process – Know Your Client, the diligence process against existing and new clients, classification of clients' AML Risk, screening of clients against sanctions lists and countries under embargo. AML Officer should appoint on staff as his/her deputy to perform daily duties in cases when AML Officer is not present in the company.

7. Responsibilities of AML Officer

AML Officer shall be responsible for:

- Preparation of Anti Money Laundering and Combating Financing Terrorism Policy;
- Monitoring and implementing AML/CFT Policy;
- Cooperation with internal auditors, external auditors and Executive Manager for issues related to AML/CFT;
- Planning and supervising the training and awareness of employees of the company for AML/CFT;
- Determining criteria for client during registering according to AML Risk;
- Conducting of annual assessment of all risks deriving from existing and new clients, new products, and services provided by the company;

8. Client Identification Process

There are two steps on client identification process:

- User Registration in the platform – it requires full legal name, date of birth, address, valid phone number, ID number, and current job title, and email.
- Realization of transaction – client must provide ID documents, and utility bill in order to verify the information provided above.

Currently, the company identifies clients through their physical presence, during costumer registering process, and through electronic platform (website) where clients can be registered, and after their registration is confirmed, can process transactions through this electronic platform.

Company verifies individual costumers' identity based on:

a) Valid identification document
b) Valid passport

In cases of conducting transactions above 10,000 Euro, company verifies individual costumers' address based on:

- Utility bill (electricity, water bill)

Company verifies legal entities' identity based on:

- Valid business certificate obtained in website: arbk.rks-gov.net.

Company verifies legal entities organizational structure based on their:

- Company Status
- Valid business certificate in website: arbk.rks-gov.net

In cases of conducting transactions above 10,000 Euro , company verifies legal entities' address based on:

- Utility bill (electricity, water bill)

Besides the above mentioned documents and processes, the company uses alternative channels of information (such as internet or social media) as source of information in order to complete client profile with the necessary data.

9. Know Your Customer (KYC) Process

The company classifies clients into individual clients and legal clients. Therefore, KYC Process for individual clients and legal clients is different and contains different requirements.

The process of Know Your Customer for individual clients serves to obtain necessary information to have a complete client profile. It contains personal identification of client, permanent or temporary address of the client, for transaction amounts above 10,000 Euro. This process is based on ID Card or Passport of the client, utility bill with the address of the client, and working contract of the client.

The process of Know Your Customer for legal clients serves to obtain necessary information for having a complete client profile. It contains identification of business and its owners, and ultimate beneficial owners, and permanent address of the business, and the main activities where the business operates and generates its income. This process is based on business certificate of legal client (which can be verified online as well: www.arbk.rks-gov.net, utility bill, and business certificate for verification of activities where the business generates its income.

Taking into consideration that company is offering services through ATM-s as well, they are used as tools for identification of clients and verification of their personal data whe service is offered through ATMs.

10. Risk classification of the clients

Taking into consideration that the risk of money laundering is assessed based on various factors, this risk is divided into three types: low risk, medium risk, and high risk. Therefore, client is categorized into one of the risk types, based on his/her profile. The risk categorization process of the client is carried on during Know Your Customer (KYC) Process.

- Low risk – client is classified with this type of risk when the profile of the client has low or does not have any indicators that may be related activities considered as vulnerable to Money Laundering/ Terrorism Financing. For example, client is a local resident and does not have any relations with PEP, his/her address is verified and is located in well known area, and client works as a teacher in local school.
- Medium risk – client is classified with this type of risk when the profile of the client contents few criteria that may be related with activities considered as vulnerable to Money Laundering/Terrorism Financing. For example, client is local resident, his/her address is verified and is located in well known area, however he is a retired PEP.
- High risk – client is classified with this type of risk when profile of the clients contents considerable criteria that may be related with activities considered as vulnerable to Money Laundering/Terrorism Financing. For example, client is foreign resident, his/her address is not permanent address, and he is parliament member.

11. Costumer due diligence

Conduction of costumer due diligence (CDD) means identification of costumer and verifying the customer's identity based on information obtained from documents and reliable sources, identification of the beneficial owner of the costumer, and obtaining information related to the purpose and nature of the relationship of costumer and the company, as well as continuous monitoring of the transactions of the costumer throughout his/her relationship with the company. Company verifies the nature of transactions and whether they are consistent with the profile of the costumer.

- Simplified costumer due diligence

Company conducts simplified costumer due diligence in cases when costumer is well known for company, as a regular costumer to whom never was detected any AML risk indicator.

Simplified costumer due diligence describes a more simplified process of information gathering, and more simplified monitoring of transactions made by customers belonging to this category.

- Customer Due Diligence

Conducting customer due diligence (CDD) means identifying the customer and verifying the customer's identity based on information obtained from documents and reliable sources, identifying the beneficial

owner of the customer, and obtaining information about the scope and nature of the relationship of the customer, as well as the continuous monitoring of the customer's transactions throughout his/her relationship with the company. The company verifies the nature of the transactions and whether they are consistent with the customer's profile.

Customer due diligence is conducted during:

- Costumer's registering process;
- Conducting transactions, when costumer wants to conduct a transaction equal to or above 10,000 Euro within 24 hours, even if costumer conducts several linked transactions that as a total are equal or passes the amount of 10,000 Euro within 24 hours;
- Conducting transactions in or from off-shore countries and countries under embargo;
- Conducting transactions with persons or entities that are under international sanctions;

- Enhanced due diligence

The company applies enhanced due diligence of costumers in the presence of a higher risk of money laundering or terrorist financing, by taking additional measures to verify or certify the documents that are obtained from client.

In execptional cases of financial relationship with costumer that is not resident of Republic of Kosovo, the company gathers sufficient information in order to fully understand the nature of its business and to determine costumer's reputation, in cases when costumer is legal entity, assesses the quality of controls in relation to combat money laundering or the financing of terrorism to which the corresponding entity is subjected, obtains additional approval from the CEO of the company whether to establish business relationship with this costumer.

12. PEP (Politically Exposed Persons) Clients

The company has risk based procedures that determine whether the costumer is a person politically exposed. These procedures include self-identification of PEP costumers and additional verification of PEP status of the costumer by AML Officer.

In cases when the company identifies a costumer as PEP customer, it classifies him/her as high risk client, obtains approval from AML Officer and CEO of the company to establish relationship with this customer, takes additional measures to establish the origin of the assets and funds used in the relationship or transaction, and ensures continuous and strengthened monitoring of the relationship with this costumer.

In these cases, the company verifies the identity of customer through documents, data or information, or other valuable source of information.

13. Screening of clients against sanctions lists

The company has in place necessary platform for screening of new and existing clients. Screening is done against the sanctions list including OFAC list of designated persons and entities, and EU sanctions lists.

Each customer's name, during onboarding process or conducting a transaction is being screened against international sanctions list. In case there is any 100% match of the name of customer with the name in the sanctions list, customer's onboarding process will be stopped, and no service will be provided to this person.

14. Verification of information

To the extend reasonable and practicable, at the time a customer relationship is established, the company will ensure, based on our assessment of the AML – related risks posed by the customer's location, nationality, and overall profile, that company has sufficient information to form a reasonable belief that we know the true identity of our customers. In verifying customer identity, company will analyze any logical inconsistencies in the information we obtain such as through documentary evidence.

The customer's identity will be verified using the information set forth above. The company is not required to take steps to determine whether any document that the customer has provided to us for identity verification has been validly issued, and the company may rely on a government – issued identification as verification of a customer's identity. However, if the company detects that the document evidences some form of fraud or other irregularities, the company will consider that the factor in determining whether it can form a reasonable belief that the customer's true identity is verified.

If a customer's identity cannot successfully be validated based on the information in the company's possession, the company may, in its sole discretion, contact the customer and request that the customer provides via facsimile:

- A true and correct copy of customer's unexpired, government – issued identification card with photograph.
- A copy of any current utility bill where the name and mailing address on the bill match the information provided by the customer.

15. Customers who refuse to provide information

If customer has questions regarding the necessity of providing identification, we will inform them it is required by regulations. If, however, a potential of existing customer refuses to provide the information described above when required, or appears to have intentionally provided misleading information, the company will not open an user for using online platform for customer, therefore will not complete the transaction with the customer, and if, after consultation with the AML Officer, it is determined to be required, the company will file a SAR (Suspicious Activity Report) to FIU.

16. Lack of verification of information

When the company cannot form a reasonable belief that company knows the true identity of a customer with respect to transactions requiring customer identification company will do the following:

- Not open user to the user on online platform of the company;
- Not perform the transaction;
- If deemed necessary or appropriate by the AML Officer, file a Suspicious Activity Report (SAR) to FIU.

17. Types of transactions

The company currently carries out the following types of transactions:

- Exchanges between FIAT and Crypto currencies in branch;
- Exchanges between FIAT and Crypto currencies through ATM;
- Exchanges between FIAT and Crypto currencies in online platform of the company;

During each crypto exchange, the company records the name, surname and crypto - receiving/sending address of the customer, as well as the crypto-currency companies that serve as intermediaries in the crypto exchange.

During the execution of FIAT (Euro)-Cryptocurrency exchanges, in cases where customers deposit values greater than 10,000 Euros in exchange for Cryptocurrencies, the customer is obliged to declare the origin of the funds through the form for declaring the origin of the funds. While ATMs offer services worth only up to 2,000 Euros, that is, below the limit of declaring the origin of the funds by the client.

18. Transaction monitoring

The monitoring of transactions is a continuous process which includes monitoring of transactions carried out by customers in the company's branches or ATMs.

Based on the results of the predefined scenarios in the monitoring platform, the transactions which are classified by this platform as transactions requiring the attention of the AML Officer, are analyzed and additional information is requested regarding their nature as well as the clients who have them. realized them. If it turns out that such a transaction is suspicious from the AML point of view, that transaction is reported to the IFI, by the AML Officer.

19. Reporting to FIU

The company has clear procedures regarding reporting of suspicious transactions to Financial Intelligence Unit of Kosovo. In the moment that one transaction of activity is considered suspicious in terms of money laundering or terrorism financing, within 24 hours is reported to FIU by AML Officer. Pursuant to Law on AML, only AML Officer has access to the list of reports submitted to FIU.

In addition to reporting suspicious transactions, the AML Officer is responsible for reporting cash transactions on a weekly basis to the Financial Intelligence Unit. Therefore, all cash transactions (deposits by the customer or cash withdrawals by the customer from the company's offices) over 10,000 Euro must be reported to the Financial Intelligence Unit.

20. Recordkeeping

Company will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancy in the identifying information.

21. Risk Assessment

The development and implementation of AML Risk Assessment must be based on a risk assessment. For this reason, the company should an AML/CTF risk assessment of the business, customers, products, and the geographic location in which it operates, in accordance with a standard risk assessment methodology.

Approved on date: 20/06/2024

Approver: