AML policy

PREAMBLE

Financial institutions and closely related entities (such as cryptocurrency exchanges) experience often attempts of money laundering and terrorist financing. In view of the fact that money laundering will undermine the development of digital asset exchange, facilitate and breed corruption, pollute social morality, damage the legitimate rights and interests of Users, destroy the foundation for the sound operation of digital assets exchanging companies, increase the legal and operational risks of digital assets exchanging companies, "Palaris" formulates these Rules in accordance with the other relevant documentation, so as to prevent money laundering and terrorist financing and fully comply with relevant regulations against money laundering and terrorist financing.

For further usage of represented terminology please, be aware that money laundering is defined as the process where the identity is disguised that it gives the appearance of legitimate income, while Terrorist financing is defined as the process of providing support to an individual or a group of terrorists. Without direct terrorist financing, such activities as fundraising, use, possession and funding arrangements also fall under the definition of terrorist financing.

According to above mentioned information "Palaris" pays thorough attention to any kind of activity that may be considered as money laundering or terrorist financing. 'Palaris" AML policy is designed to prevent money laundering by complying with FIU AML legislation obligations, including the need to have adequate systems and controls in place to mitigate the risk of being used to facilitate the financial crime. To minimize and mitigate the risk of money laundering and/or terrorist financing, "Palaris" implemented effective internal measures and procedures:

- Establishment of the identity of Palaris customer;
- Assessment of risk;
- Monitoring of the customer's activities; and internal control
- Reporting of suspicious activities to respective authorities.

General requirements of the company

Before the Company can execute any transaction for any new client, a number of procedures need to be in place and carried out:

- AML/KYC procedures
- including customer identification,
- record-keeping,
- discovering and monitoring of unusual or suspicious transactions
- internal/external reporting and control;

Establishment of the identity

For individual users

For "Palaris" to be able to establish the identity of its customer, we must obtain sufficient data/documents/information from a customer and verify such data/ documents/ information against independent sources. This kind of information could be personal information: your name, address (and permanent address, if the two are different)[1], date of birth and nationality, valid photo, contact information as a telephone/mobile phone number, valid email address and other information available[2]. Identity authentication shall be based on documents issued by the official or other similar authorities, such as passports, identity cards, or other identity documents as are required and issued by relevant jurisdictions.

For institutional users

For "Palaris" to be able to establish the identity of its institutional users, we must obtain sufficient data/documents/information from a customer and verify such data/ documents/ information that could be: name of the institution; registered office address of the institution; contact information of the institution; articles of association of the institution; description of the equity structure and ownership of the institution; legal representative of the institution; place of residence of the legal representative of the institution; contact information of the legal representative of the institution; the institution's business license; the institution's consent to open an account with this Platform; letter of authorization by the institution; a copy of the valid Identity Card or a valid passport of the legal representative of the institution; and other information or documents to be provided upon request by the company.

Submission and Review of user Documents

The company will verify and record the relevant information submitted by the individual/institutional users in accordance with the user identification system under the platform's relevant regulations against money laundering. If the Platform has any doubt about the information submitted by any User, it has the right to ask the User to provide other documents or consult with relevant competent authorities or departments for verification.

Re-establishment of the identity

Palaris retains a right to re-establish the identity of the customer in cases where Palaris sees it fit and in relation to that, request additional data/documents/information or renew previously submitted.

The customer's identification information will be collected, stored, shared and protected strictly in accordance with Palaris Privacy Notice and related regulations.

---

[1] The address you provide will be validated in an appropriate manner, such as checking the fare ticket of the means of transportation you use, your interest rate bills, or voter registration.

[2] We may request you to provide further information under circumstances to meet our KYC and AML obligations under relevant laws and regulations.

Assessment of risk

To mitigate and minimize the risks, Palaris has adopted a risk-based approach which enables to identify, assess and understand the money laundering and terrorist financing risk to which Palaris is exposed and take the appropriate mitigation measures in accordance with the level of risk.

According to the risk-based approach Palaris classifies users into three categories, i.e., low-risk Users, medium-risk Users and high-risk users according to the materials submitted by the users, and on the basis of such factors as the geographical location of the users, the industries they are involved in, background of the shareholders of users, if any, and whether users are prominent public figures, *inter alia*.

High-risk Users

High-risk users refer to users who comprise any of the following high-risk factors and are identified as high-risk users after a comprehensive evaluation by the Platform. High-risk Users include:

- Users who have been subject to or are currently under criminal or administrative investigation, excluding Users who are investigated in connection with any civil proceeding or emergency dispute;
- Users who are prominent public figures, or whose controlling shareholders, actual controllers and/or actual beneficiaries are prominent public figures;
- Users who are from high-risk countries or regions, or their controlling shareholders, actual controllers and/or actual beneficiaries are from high-risk countries or regions;
- Users who are identified as key suspicious Users according to relevant procedures of the Platform;
- Users who are engaged in business operations in industries subject to a relatively high level of money laundering risks, such as jewelry, precious metals trading, currency exchange, pawn brokerage, money remission, nightclubs and the arms industry, etc;
- Users who engage in intensive trading within a certain period of time, which is seriously inconsistent with the situation on the digital assets markets; and
- Users who engage in unusual operations.

Customers that in the opinion of Palaris pose higher risk may be investigated more thoroughly which may result in the request of additional information and taking longer term for verification of the identity of such customer. customers or industries that are subject to EDD require enhanced customer due diligence measures, which may involve:

- Obtaining additional identification materials
- Establishing the source of funds or wealth
- Closer scrutiny of the nature of the business relationship or purpose of a transaction
- Implementing ongoing monitoring procedures

Low-risk Users

Low-risk Users refers to those Users who are identified as low-risk Users after a comprehensive evaluation by the Platform. Low-risk factors include:

- Users that are financial institutions or well-known companies;
- Users who are natural person and of whom the Platform has proper understanding through verification and who carry a relatively low risk of money laundering;
- Users who are reviewed and approved by the Platform's risk control and compliance departments.

Medium-risk Users

Medium-risk users refers to users other than those specified under the name "high risk " and "low risk users" reflected in these Rules.

Monitoring

To get to know our customers, Palaris performs ongoing and retrospective monitoring. Monitoring performed by Palaris intends not only to get to know the customer, but also to notice unconformities in comparison to information submitted to Palaris by the customer or obtained by Palaris during the establishment of the customer's identity.

We also monitor activities used within Palaris services in order to catch any attempts of fraudulent, illegal or unlawful activity. Palaris uses both manual and automatic solutions in order to track the customer's transactions. Palaris may use other measures on case by case basis. Each suspicious activity will be thoroughly investigated and, if necessary, reported by Palaris MLRO to the respective authorities or other restrictive measures will be taken in order to ensure no money laundering or terrorist financing activity is performed. Palaris is entitled to request additional information/data/documents in relation to any transaction and the customer must follow such request.

Ongoing monitoring involves:

• Monitoring transactions throughout the course of relationship to ensure a client's risk profile matches their behavior.

• Maintaining responsiveness to any changes in risk profile, or any factors which might raise suspicion.

• Keeping relevant records, documents, data and information that may be needed for customer due diligence purposes.

KYC Enhanced Due Diligence is specifically designed for dealing with high-risk or high-net worth customers and large transactions. Since these customers and transactions pose greater risks to the financial sector, they are heavily regulated and monitored in order to ensure that everything is above board. Palaris EDD policies significantly require more evidence and detailed information to be collected. The entire process of EDD is documented in detail in order for the regulators to be able to have immediate access to the data.

Reporting to the authorities

Following its AML Policy and the applicable legal acts, Palaris, when necessary, will report to the respective authorities of the activities that may be considered as money laundering and terrorist financing. Palaris will not disclose any information about such report which has been made and will not address any questions in relation to that. Palaris MLRO is involved in designing relevant policies and procedures, record-keeping, filing internal and external reports and ensuring due diligence is performed on customers.

Our MLRO also participates in the ongoing review of Palaris internal policies, procedures and professional relationships, in order to ensure that money laundering and other financial crimes are detected and reported in compliance with the law. Palaris money laundering reporting officer provides training to colleagues within the company.

Compliance officer

Palaris has the assigned compliance officer who is responsible for implementation of Palaris AML policy, including but not limited to, of the above listed activities. While all Palaris employees are aware of the company's AML policy, our Compliance Officer is responsible for its implementation. The Compliance Officer focuses on the internal systems and makes sure all documentation is in place to help detect, monitor and report money laundering activities to the authorities.

Palaris compliance officer includes the following policies and strategies:

• Assisting with the development, implementation and maintenance of an anti-money laundering program within Palaris company.

• Ensuring compliance with current AML regulations and other relevant legislations.

• Developing and maintaining a risk assessment framework for products and services, customers and other issues relating to money laundering.

• Keeping and maintaining records of customers and reporting suspicious activities to the authorities.

• Arranging and implementing inspections and audits from third-party organizations and making compliance recommendations based on the findings.

• Briefing and reporting to senior management on matters relating to internal AML compliance policies and procedures.

• Overseeing and implementing an ongoing AML training program for all employees.