KYC/AML POLICY

Introduction

Capitual's Anti-Money Laundering and Know Your Customer Policy, hereinafter referred as THE KYC/AML POLICY, is designed to prevent and mitigate possible risks of Cryptostream OU, registered in Estonia under the registration number 14437172, hereinafter referred as "Capitual", being involved in illegal activities of any kind.

Local and international laws require Capitual to implement effective internal procedures and mechanisms that prevent illegal activities, such as money laundering, terrorist financing, drugs trafficking, human trafficking, proliferation of weapons of mass destruction, corruption and bribery. These regulations also require from Capitual an incident response in case of any suspicion activity from one or more of its users.

This KYC/AML POLICY covers the following matters:

1. Verification procedures;

2. Compliance Team;

3. Transactions monitoring;

4. Risk Assessment.

1. Verification procedures

Capitual follows the international standard for preventing illegal activity named Customer Due Diligence ("CDD"), which means that Capitual establishes its own verification procedures that do follow international agreements of anti-money laundering and "Know Your Customer" (KYC) frameworks.

1.1. Identity verification

Capitual's identity verification procedure requires the User to provide Capitual, with reliable and independent sources, data or information (e.g. national ID, international passport). For such purpose, Capitual reserves rights to collect provided User's identification information for the KYC/AML POLICY purposes.

To the provided documents, Capitual takes steps to confirm their authenticity, as well as compare with the information provided by the User. This is done in a two-

steps procedure, where the first step is performed by an internal Artificial Intelligence and Machine Learning-powered automatic system and the second step is performed by human beings at the Compliance Team.

All legal methods for double-checking identification information can be used. Capitual reserves the right to investigate Users who have been appointed by automatic or manual verification to be risky, suspicious or possibly harmful, and to require from the User or third-parties' sources any additional documents or information that may be needed for the purposes of the investigation.

Capitual also reserves the right to repeat the verification steps at any time and at an on-going basis, or on a triggered-basis, such as when the user's identification information has been changed or their activity seemed to be suspicious or out of the User's standards, as well as to put automated machine learning models to warn the Compliance Team when the User's activities should be checked. Additionally, Capitual reserves the right to request up-to-date documents from the User, regardless of them having passed the identity verification procedure in the past.

User's documents and information will be collected, safely stored, protected and, when required by official agencies, shared, in strict accordance with Capitual's Privacy Policy and official regulations, the latter prevailing in case of conflict.

Capitual removes itself from potential legal liability in a situation where its offered services have been used by identity-verified users to conduct illegal activities.

2. Compliance Team

The Compliance Team is the team managed by the Compliance Officer, under duly authorization by Capitual, to ensure the effective implementation and enforcement of this KYC/AML POLICY. It is their responsibility to supervise and ensure the execution of all aspects defined in Capitual's KYC/AML POLICY in order to avoid anti-money laundering and counter-terrorist financing, including, but not limited to:

1. Collecting needed User's identification information;

2. Establishing and keeping up-to-date internal policies and procedures for completion, review, submission and retention of all reports and records required, under the applicable regulations;

3. Monitoring transactions and investigating any significant deviations from Users' standards;

4. Implementing, with the Development Team, records management for appropriate storage and retrieval of documents, files and logs;

5. Updating risk assessment regularly, as well as keeping updated local copies of recognized “black lists” (e.g. OFAC’s SDN List) and checking Users list for the presence of any individual or corporation present on these lists, and initiating investigation, with official agencies, that may or may not lead to the account’s suspension;

6. Providing law enforcement with information as required under the applicable laws and regulations.

The Compliance Team interacts with law enforcement, which are involved in prevention of money laundering, terrorist activities financing and other illegal activities.

3. Transactions Monitoring

Users are known not only by their identity verification (“who they are”), but, more importantly, by analyzing their activities patterns (“what they do”). For this reason, Capitual relies on data analysis as a risk-assessment and suspicion detecting models. Capitual performs, continuously, several compliance-related tasks, including, but not limited to capturing data, filtering, keeping activities records, investigation management and, when needed, reporting.

Capitual automated verification procedures include:

1. Daily check of Users against recognized “black lists” (i.e. OFAC SDN List), aggregating transfers by multiple data points, placing Users on watch and service denial lists, opening cases for investigation where needed, sending internal communications and filling out statutory reports, when applicable;

2. Case and document management.

With regard to this KYC/AML POLICY, Capitual will monitor all transactions and reserves the rights to:

1. Ensure that transactions of suspicious nature are reported to the proper law enforcement through the Compliance Team;

2. Request the User to provide any additional information and documents in case of suspicious transactions;

3. Suspend or terminate User's Account when Capitual has reasonably suspicion that the User is engaged in illegal activity.

As the above list is not exhaustive, the Compliance Team will monitor User's transactions on a day-to-day basis, in order to define whether one's transactions are to be reported and treated as suspicious or are to be treated as *bona fide*.

4. Risk Assessment

Capitual follows international anti-money laundering and terrorists financing requirements, and has adopted a risk-based approach to prevent or mitigate such illegal activities, ensuring that these measures are commensurate to the identified risks.

This approach allows resources to be allocated in the most efficient ways, under the principle that preaches that resources should be directed in accordance with priorities, so that the greatest risks receives highest attention.