

Last updated: May 07, 2020

Introduction

As a virtual currency service provider of virtual currency wallet services and virtual currency exchange services, HODLTech OÜ is committed to establishing and maintaining policies, controls and procedures that mitigate the risks of money laundering and terrorist financing (collectively, the "**Policies**"). These Policies are reviewed frequently and amended from time to time based on prevailing industry standards and international regulations designed to facilitate the prevention of illicit activity including money laundering and terrorist financing. Due diligence is conducted on our customers, clientele, contributors, and other contacts with which HODLTech OÜ has any financial dealings with (collectively, "**Clients**") to ensure compliance with all applicable laws and regulations.

Money Laundering Risks

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Terrorist financing is an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes.

AML/KYC Policies Framework

The Policies are designed to lay down a framework to:

- enable HODLTech OÜ to know and understand its Clients and their background and source of funds better, which in turn will help it manage its risks prudently;
- prevent HODLTech OÜ from being used, intentionally or unintentionally, by criminal elements for illicit activity including money laundering or financing terrorist activities;
- put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws, procedures and regulatory guidelines; and
- equip employees and contractors of HODLTech OÜ with the necessary training and measures to deal with matters concerning KYC/AML procedures and reporting obligations.

Risk-Based Approach

HODLTech OÜ takes a risk-based approach ("**RBA**") towards assessing and containing the money laundering and terrorist financing risks arising from any transactions it has with Clients and uses all available data when reviewing Client activity.

Before entering into any transaction or proposed transaction, necessary checks shall be conducted in line with the RBA so as to ensure that the identity of the Clients does not match with any person with a known criminal background or with banned entities such as individual terrorists or terrorist organizations. Enhanced due diligence would be required for higher-risk Clients, especially those for whom the sources of funds are not clear, or for transactions of higher value and frequency, which shall be determined by HODLTech OÜ in its sole and absolute discretion.

Know Your Client; Client Identification

HODLTech OÜ requires its Clients to undergo Know Your Customer (KYC) checks, including, without limitation, identity verification which may consist of the Client providing:

- a high-resolution, clearly readable, non-expired copy of the Client's government-issued ID or IDs (passport, national identity card and/or a driver's license);
- a unique photo of person holding his/her government-issued ID(s) as well as a unique handwritten note;
- a video conference with or statement from the Client; and
- clearly readable proof of residential address is required by obtaining a copy of an acceptable address proof document not older than 3 months old. The document must carry the Client's name and address (recent utility bill or bank statement).

Care must be taken that all documents provided are true copies of the original.

Providing false, forged, modified or documents meant to deceive is considered fraud and will be treated as such. All assets derived from fraudulent transactions and/or suspicious activity may be seized and forfeited. Such activity may also be reported to the relevant authorities.

HODLTech OÜ may decide to use the following non-documentary methods of verifying identity:

- independently verifying the Client's identity through the comparison of information provided by the Client with information obtained from a consumer reporting agency, public database or other source;
- checking references with other institutions;
- analyzing whether there is logical consistency between the identifying information provided, such as the Client's name, street address, postal code, and date of birth;
- utilizing complex device identification (such as "digital fingerprints" or IP geolocation checks); and
- obtaining a notarized or certified true copy of an individual's birth certificate or government-issued ID for valid identification.

When there shall be any suspicion of illicit activity including money laundering or terrorism financing activities, or where there shall be any doubt about the adequacy or veracity of previously obtained Clients' identification data, further due diligence measures shall be undertaken, including verifying the identity of the Client again and

obtaining information regarding the purpose and intended nature of the relationship with HODLTech OÜ.

High-Risk Jurisdictions; Sanctions; Politically Exposed Persons

HODLTech OÜ does not serve Clients from certain regions that are deemed high-risk or unwelcoming from a legal or regulatory perspective, including Cuba, Iran, North Korea and Syria.

Various global sanction lists are also checked when carrying out due diligence and identity verification of Clients. Where there may be a reason for suspicion or a potential match to any sanctions list, enhanced due diligence measures will be applied. HODLTech OÜ does not open accounts or transact with individuals that are on prescribed sanctions lists.

HODLTech OÜ does not open accounts or transact with individuals who are Politically Exposed Persons (PEPs), or their family members. HODLTech OÜ screens all Clients against global PEP lists before they are allowed to establish a relationship with HODLTech OÜ.

Compliance Officer

The Compliance Officer is the person, duly authorized by HODLTech OÜ, whose duty is to ensure the effective implementation and enforcement of the AML/KYC Policy. It is the Compliance Officer's responsibility to supervise all aspects of HODLTech OÜ's anti-money laundering and counter-terrorist financing initiatives, including but not limited to:

- collecting Clients' identification information;
- establishing and updating internal policies and procedures for the completion, review, submission and retention of all reports and records required under the applicable laws and regulations;
- monitoring transactions and investigating any significant deviations from normal activity;
- implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs;
- updating risk assessment regularly; and
- providing law enforcement with information as required under the applicable laws and regulations. The Compliance Officer is entitled to interact with law enforcement, which are involved in prevention of money laundering, terrorist financing, and other illegal activity.

Ongoing Due Diligence; Monitoring and Reporting

HODLTech OÜ diligently monitors transactions for suspicious activity and must conduct ongoing due diligence on existing Clients. Any Client activity outside normal or expected activity may be considered unusual and enhanced due diligence measures will be applied. Understanding the Client profile is crucial to assessing potential indicators of suspicious activity. An investigation into suspicious activity will try to establish the true motivation behind the activity in question. This may result in confirmation of the suspicious activity or removal of reasonable doubt. If suspicious activity is confirmed, the issue will be escalated accordingly both internally and externally.

When such suspicious activity is detected, the Compliance Officer will determine whether a filing with any law enforcement authority is necessary.

Termination of Services

HODLTech OÜ reserves the right to deny or terminate servicing a Client or account at any time in line with the Policies and HODLTech OÜ's User Agreement (<https://hodltech.eu/ua.pdf>) should suspicion arise that a Client is involved with or connected with money laundering, criminal activity, terrorist financing or any other predicate offense to money laundering or terrorist financing. HODLTech OÜ will not enter into any business arrangement with anyone or group suspected of or involved in criminal activity including money laundering or terrorist financing.