

MASTERNODED AML POLICY

AML Policy

Anti-Money Laundering Policy (AML Policy)

Money laundering is the disguising of an illegal source of funds by converting it to cash or investments that are ostensibly legitimate.

General provisions

This Anti-money Laundering Policy (hereinafter referred to as "AML Policy") outlines the procedures and mechanisms used by MasterNoded for the purpose of preventing money laundering. MasterNoded adheres to the following policies:

- not entering into business relationships with criminals and/or terrorists;
- not processing transactions that are result from criminal and/or terrorist activities;
- not facilitating any transactions related to criminal and/or terrorist activities;

Verification Procedures

MasterNoded shall establish its own procedures for determining compliance with the anti-money laundering standards and Know Your Customer (KYC) policy.

MasterNoded Customers complete a verification procedure (they must provide an identification document issued by the state: passport or an ID card). MasterNoded reserves the right to collect Customers' identification information for AML Policy purposes. This information is processed and stored strictly in accordance with the MasterNoded Privacy Policy.

MasterNoded may also request a second Customer identification document: a bank statement or utility bill no older than 3 months, which includes the Customer's full name and current address.

MasterNoded shall verify the authenticity of documents and information provided by Customers and reserves the right to request additional information on Customers who have been identified as dangerous or suspicious.

If the Customer's identification information has been changed or their activity appears suspicious, MasterNoded is entitled to request updated documents from the Customer, even if they have been authenticated in the past.

Anti-Money Laundering Officer

The Anti-Money Laundering Officer is a MasterNoded employee who is responsible for ensuring compliance with the AML Policy, such as:

- collection of Customers' identity information;
- establish and update internal policies and procedures for creating, reviewing, submitting and storing all reports required in accordance with existing laws and regulations;
- transactions monitoring and analysis of any significant deviations from the Customers' usual activities;
- the introduction of a records management system for storing and retrieving documents, files, forms and logs;
- regularly update risk assessments.

An Anti-Money Laundering Officer has the right to engage with law enforcement agencies that deal with the prevention of money laundering, financing of terrorism and other illegal activities.

Transactions Monitoring

The monitoring of the Customer's transactions and the analysis of the obtained data is also a tool for risk assessment and the detection of suspicious transactions. If money laundering is suspected MasterNoded shall monitor all transactions and reserves the right to:

- reporting of suspicious transactions to the relevant law enforcement agencies;
- request the Customer to provide any additional information and documents;
- suspend or terminate the Customer's Account.

The above list is not exhaustive. The AML Policy Compliance Officer monitors the Customers' transactions every day to determine whether to report them and treat them as suspicious.

Risk assessment

In accordance with international requirements, MasterNoded applies a risk-based approach to anti-money laundering and financing of terrorism. Thus, measures aimed at the prevention of money laundering and financing of terrorism are commensurate with the identified risks, allowing resources to be effectively dedicated. Resources are used on a priority basis; the greatest attention is given to the greatest risks.