

ANTI-MONEY LAUNDERING AND KNOW-YOUR-CUSTOMER POLICY

(AML & KYC)

Last updated on 21 August 2024

<https://www.tailcor.com/> website (hereinafter the “Website”) is operated by TAILCOR LIMITED LIABILITY COMPANY (hereinafter the “Company”, “we”, “us”, “our”) that conducts business in accordance with the anti-money laundering/counter-financing of terrorism legal framework (AML/CFT) to protect the funds of our clients and assure compliance with AML standards. As a regulated business, the Company has adopted this Anti-Money Laundering Policy (“AML Policy”).

Definitions.

AML (anti-money laundering) - a set of activities, procedures, and regulations designed to prevent criminal activities related to money laundering;

CFT (combating the financing of terrorism) - a set of activities, procedures and regulations created in order to prevent criminal activities related to terrorism;

Financing of terrorism - a crime against public safety consisting in collecting, transferring, or offering property values in order to finance a terrorist crime or making property values available to a person, an organized group aimed at committing such an offense (in detail the act specified in Article 165a of the Act of 6 June 1997 Criminal Code);

GIIF - General Inspector of Financial Information, a government administration body responsible for counteracting money laundering and terrorist financing;

Obligated institution - entrepreneurs, companies and institutions that are obliged to analyze transactions and provide the GIIF with information on suspicious transactions;

Clients - natural person, to whom the Company provides services or for whom it performs activities falling within the scope of its professional activity (including with whom organization establishes economic relations or on whose behalf it carries out occasional transaction);

Politically Exposed Person (hereinafter PEP) - an individual who holds a significant position or public office;

Employee - a natural person performing duties for the obliged institution (the Company) regardless of the legal form on the basis, of which the cooperation was established (employment contract, contract of mandate, cooperation agreement and others);

Money laundering - an activity aimed at introducing to the legal turnover of money originating from illegal sources or used for financing illegal activity (in detail, the act specified in Art. 299 of the Act of 6 June 1997 - Criminal Code);

Transaction - a legal or factual act by which ownership or possession of property values is transferred, or a legal or factual act performed for the purpose of transferring ownership or possession of property values.

Purposes and basis.

The purpose of this AML & KYC Policy is to introduce in the obliged institution financial security

measures and other obligations stipulated by the regulations, in accordance with the Law on Anti Money Laundering and Financing of Terrorism. Since the aim of the obliged institution is to operate transparently, in accordance with the law and the principles of social coexistence, this AML & KYC Policy is intended to prevent the use of its services in an unlawful manner.

Scope of application.

This AML & KYC Policy applies to all Clients trading on the Website. By creating an account on our Website, the Client voluntarily and fully acknowledges the Company's AML Policy and agrees to abide by its AML and KYC procedures.

AML measures.

The Company sets the following AML measures:

- Before entering a business relationship, the client's identity must be verified.
- Implementing and maintaining risk-based client due diligence, including enhanced due diligence for clients who pose higher risks.
- Transaction monitoring based on the risk analysis.
- Reporting suspicious activity internally, and to the relevant authorities if required by applicable laws and regulations.
- Regular AML training for our team.

KYC procedures.

The Company has established Know Your Customer (KYC) procedures to combat money laundering and the financing of terrorism. These procedures allow us to identify every Client that we deal with, to understand the legitimacy of our business relationships, and to identify and react to unusual or suspicious activity.

Purposes of KYC.

By collecting and reviewing Client data, the Company commits to:

- establishing the identity of our Clients;
- checking that our Clients are not considered high-risk;
- monitoring transactions for unusual or suspicious activity - this type of activity will cause the Client to be considered high-risk.

Client's Due Diligence.

In accordance with our KYC policy and procedures, the Company can require and verify the authenticity of identification data, contact data, and financial data from its Clients.

Simplified Due Diligence.

Simplified due diligence measures may be applied where a risk assessment confirms a lower risk of money laundering or terrorist financing.

Enhanced Due Diligence.

Enhanced due diligence measures shall apply where there is a higher risk of money laundering or terrorist financing, and in particular, in the case of customers from or established in a high-risk third country. Enhanced due diligence measures may consist, in particular, in verifying the customer with more than one of the required documents.

Client's Identity verification.

The Client is required to provide:

- a) full name, (and document that confirms the identity)
- b) state-assigned identification number (supported by documents such as photocopy of national ID, international passport, or other ID documents),
- c) date of birth,
- d) nationality,
- e) telephone number,
- f) email,
- g) address (supported by documents such as a bank statement and utility bill as proof of address),
- h) other information or documents requested by the Company (photo of the Client, documents confirming the source of funds, etc.).

Sanctions and PEP lists screening.

PEPs may constitute an additional factor of risk. The Company screens Clients against Sanctions and Politically Exposed Persons (PEPs) lists by using such tools as KYCAID and our own software. PEPs are subject to enhanced due diligence.

Jurisdiction Restrictions.

Client domicile is considered one of the factors associated with customer risk analysis. The Company provides verification of the country of residence of the Client with respect to:

- degree of corruption (clash with corruption maps)
- deviation of the place of residence or domicile from the usual customer
- residence in a tax haven (countries applying harmful tax competition)
- origin from high-risk countries designated by the European Commission and FATF or recognized as such by the obliged institution, whereby as of the date of introduction of the procedure is meant at least:

[Banned countries](#). Clients and traffic from the following countries are banned from use of Company services:

- Afghanistan
- Belarus
- Burundi

- Burkina Faso
- Cambodia
- Central African Republic Sanctions
- Crimea, Donetsk, Lugansk, Kherson regions of Ukraine
- Cuba
- Democratic People's Republic of Korea (DPRK)
- Iran
- Iraq
- Jordan
- Lebanon
- Libya
- Myanmar
- Russia
- Panama
- Senegal
- Somalia
- South Sudan
- Sudan and Darfur
- Syria
- Tanzania
- Trinidad and Tobago
- Vanuatu
- Venezuela
- Yemen
- Uganda
- United Kingdom

[Grey/high-risk countries](#). Clients from these countries have to verify their ID before they can send out or sell cryptocurrency:

- Barbados,
- Bulgaria,
- Burkina Faso,
- Cameroon,
- Democratic Republic of Congo,
- Croatia,
- Gibraltar,
- Haiti,
- Kenya,
- Jamaica,
- Mali,
- Mozambique,
- Nigeria,
- Philippines,
- Senegal,
- South Africa,
- South Sudan,
- Syria,
- Tanzania,
- Türkiye,
- Uganda,

- United Arab Emirates,
- Vietnam,
- Yemen

Client's transactions.

If the seizure of transactions is inconsistent with the client's business profile, it should be included in the risk assessment. The company can request proof of the source of funds, the purpose and the intended nature of the transaction. Bank account number, and credit/debit card information are needed for the card verification process only.

Low-risk Clients.

Low risk may be indicated by the fact that the Client is:

- a) A resident of a member state of the European Union, a member state of EFTA - a party to the EEA Agreement,
- b) A resident of a third country that is determined by reliable sources to be a country with a low level of corruption or other criminal activity,
- c) Resident of a third country where according to reliable sources AML/CFT regulations are in force.

High-risk Clients.

High risk occurs in particular when:

- a) The Company doubts the authenticity, validity and/or integrity of the Client's identity information;
- b) The Client is from or based in a high-risk third country,
- c) The Client has a PEP status,
- d) The transaction has the status of an unusual transaction,
- e) Suspicious conduct on the part of the Client.

Termination of services.

If Clients are considered high-risk for any reason (e.g., high-risk jurisdiction, false documents, discrepancies in provided information, payments from questionable sources, e.g., when details of the Client and the account holder do not match, suspicious activity, PEP or sanction lists) the Company reserves the right to reject the client's documents, to request for additional documents and information, cancel any payments and transfers, block or close the account.

Compliance Officer.

The management board of the Company has appointed AML officer, whose responsibilities include gathering and studying data on transactions and circumstances that may be related to money laundering or terrorist financing, implementing statutory regulations, ensuring compliance with the activities of the obligated institution and its employees and other persons performing activities for the entity, providing notifications of statutory requirements, reporting to the authorities in the event of

suspicion of money laundering or terrorist financing, introducing employees' education and training program.

Confidentiality.

Any Company employee who obtains information relating to anti-money laundering while performing their duties related to money laundering must strictly adhere to confidentiality obligations and maintain the privacy of all Client's information. All Client's data are collected and stored in accordance with our Privacy Policy and applicable laws and regulations.

Information requests.

For more information on this AML & KYC Policy, please contact us at info@tailcor.com.