AML POLICY

Last updated: 11.05.2026

SPEEND.IO ("Speend", the "Company") is committed to upholding high standards of integrity, transparency, and compliance with applicable legal and regulatory requirements and recognized international AML/CFT standards. Speend.io maintains a zero-tolerance approach to money laundering, terrorist financing, sanctions evasion, fraud and any other form of unlawful or illicit activity.

We are committed to implementing policies, procedures, and internal controls based on recognized industry practices and effective international anti-money laundering standards. We understand the importance of preventing money laundering and take appropriate measures to ensure that our services are not used for fraudulent, illegal, or other prohibited purposes.

This Anti-Money Laundering (AML) and Know Your Customer (KYC) Policy sets out our commitment to combating financial crime and ensuring the legitimacy of transactions carried out through our platform.

1. PURPOSE OF THIS DOCUMENT

The purpose of this document is to offer a concise overview of the elements and procedures within the Company's Anti-Money Laundering/Counter-Terrorist Financing (AML/CTF) compliance regime. It is intended to provide insight to the Company's partners, clients, vendors, contractors, employees, regulators, law enforcement, and other stakeholders concerned with our AML/CTF efforts.

2. THE COMPANY DEFINES MONEY LAUNDERING:

1. The act of converting or transferring property, with the knowledge that said property originates from criminal activity or active involvement in such unlawful actions, to conceal or disguise the illegal origin of the property. This may also include assisting any individual engaged in such activities to evade the legal consequences of their actions.
2. The act of concealing or disguising the genuine nature, source, location, disposition, movement, rights associated with, or ownership of property, with the knowledge that such property is derived from criminal activity or active involvement in such activity.
3. The act of acquiring, possessing, or utilizing property, with awareness at the time of receipt that the mentioned property was derived from criminal activity or active involvement in such activity.
4. Participation in, association with the intent to commit, attempts to commit, and aiding, abetting, facilitating, and counseling the commission of any of the actions described in points 1, 2, and 3.

Terrorist financing involves the provision of funds for terrorist activities. Legally, it encompasses the act of acquiring or gathering funds, through any means, either directly or indirectly, with the intention that these funds will be used, or with the knowledge that they will be used, either in whole or in part, to facilitate any form of terrorism.

Terrorist activities primarily aim to intimidate a population or coerce a government into specific actions. This is achieved through deliberate acts such as intentional killing, causing severe harm or endangering individuals, inflicting significant property damage that has the potential to cause serious harm to people, or substantially interfering with or disrupting essential services, facilities, or systems.

Speend.io is required to comply with applicable anti-money laundering, counter-terrorist financing, counter-proliferation financing and sanctions requirements, including Costa Rican Law No. 7786 — Law on Narcotic Drugs, Psychotropic Substances, Unauthorized Drugs, Related Activities, Money Laundering and Terrorist Financing, as amended, including, where applicable, obligations under Article 15-bis of Law

No. 7786 and related AML/CFT rules, regulations and guidance issued by competent Costa Rican authorities, including SUGEF.

Speend.io also operates in accordance with applicable international AML/CFT and sanctions standards, including but not limited to:

1. Financial Action Task Force (FATF) Recommendations, including recommendations and guidance applicable to virtual assets and virtual asset service providers;
2. United Nations Security Council sanctions regimes and applicable UN sanctions lists;
3. United States sanctions requirements, including sanctions administered by the Office of Foreign Assets Control of the U.S. Department of the Treasury (OFAC), where applicable;
4. European Union restrictive measures and sanctions regulations, where applicable;
5. United Kingdom sanctions requirements, including sanctions administered by HM Treasury / OFSI, where applicable;
6. other applicable national and international AML/CFT, sanctions, anti-bribery, anti-corruption and counter-terrorist financing laws, regulations and guidance.

These requirements may include identifying and verifying clients' identities, conducting customer due diligence and enhanced due diligence where required, screening clients, beneficial owners, counterparties and transactions against applicable sanctions, PEP and adverse media databases, carrying out ongoing monitoring of client activity, including transaction monitoring, maintaining records of clients' activity and related documents, and reporting suspicious or reportable transactions to competent authorities where required.

Our compliance with applicable AML/CFT, sanctions and counter-terrorist financing laws, regulations and standards is mandatory.

3. RISK-BASED APPROACH AND RISK ASSESSMENT

At Speend.io, we apply a risk-based approach to our due diligence procedures. This includes collecting and reviewing relevant information and documents to assess the risk profile of each prospective client. Our team applies due care, professional judgment, and a thorough review process to evaluate the nature, background, and activity of all clients.

Speend.io is committed to conducting its business in accordance with high ethical and compliance standards. We do not enter into business relationships with individuals or entities that may expose the Company to reputational, legal, regulatory, financial crime, or other material risks, or that may negatively affect the integrity of the virtual currency industry.

For the purpose of identifying, assessing, and analyzing money laundering and terrorist financing risks related to its activities, the Company conducts a risk assessment taking into account, among others, the following risk categories:

- customer risk;
- geographical risk;
- product and service risk; and
- delivery channel risk.

Once the risk level is assessed and assigned to a particular customer, it shall be reviewed periodically, depending on the degree of risk, the customer's profile, and the nature of the customer's activity.

Compliance Officer

The management body of the Company shall appoint a Compliance Officer responsible for overseeing and coordinating the Company's AML/CTF compliance framework and related internal procedures.

The Compliance Officer shall act as the main internal contact person for AML/CTF, sanctions, customer due diligence, transaction monitoring and suspicious activity escalation matters. Where required under applicable Costa Rican laws and regulations, the Compliance Officer may also act as the contact person for competent authorities, regulators, financial intelligence authorities, banks, payment providers, crypto service providers and other relevant counterparties.

The Compliance Officer shall report directly to the management body of the Company and shall have sufficient authority, independence, resources and access to relevant information across the Company's business operations to properly perform their duties.

Only a person with appropriate education, professional competence, experience, personal qualities and good reputation may be appointed as the Compliance Officer.

The duties of the Compliance Officer include, among others:

- organizing and overseeing the collection, review and analysis of information relating to unusual, suspicious or high-risk transactions, customers, activities or circumstances identified in the course of the Company's operations;
- overseeing customer due diligence, enhanced due diligence, ongoing monitoring, sanctions screening and transaction monitoring procedures;
- escalating internally any suspicion of money laundering, terrorist financing, sanctions evasion, fraud or other illicit activity;
- where required by applicable Costa Rican laws and regulations, preparing and submitting reports, notices or other communications to the competent authorities;
- periodically reporting to the Company's management body on the Company's AML/CTF compliance framework, identified risks, suspicious activity, internal controls and compliance with applicable legal and regulatory requirements;
- maintaining relevant AML/CTF, sanctions, customer due diligence and transaction monitoring records;
- supporting the review and update of the Company's AML/CTF policies, procedures and internal controls;
- performing other duties and obligations related to the Company's compliance with applicable AML/CTF, sanctions and financial crime prevention requirements.

4. AML COMPLIANCE PROGRAM

4.1. Due Diligence

The Company applies the following due diligence measures:

- identification of a customer and verification of the submitted information based on information obtained from a reliable and independent source, including using means of electronic identification and trust services for electronic transactions;
- identification of the beneficial owner and, for the purpose of verifying their identity, taking measures to the extent that allows the Company to make certain that it knows who the beneficial owner is, and understands the ownership and control structure of the customer;
- understanding of business relationships, and, where relevant, gathering information thereon;
- verification of information on whether a person is a politically exposed person, their family member, or a person known to be a close associate;
- sanction screening of its customers;

- monitoring of a business relationship.

4.2. Transaction Monitoring
We employ sophisticated transaction monitoring systems to detect and report suspicious activities.

Customer's transaction pattern is monitored to detect unusual or suspicious transactions. Speend.io will therefore monitor all transactions and it reserves the right to request additional information from customers where transactions seem suspicious and report all suspicious transactions to the relevant authorities through its Compliance officer. Speend.io will make regular Suspicious transaction reports to the relevant authorities in cases they arise.

The compliance officer will carry out daily monitoring of all transactions to determine which transactions are legitimate and which seem suspicious. Suspicious/ Unusual transactions are reported to the relevant authorities.

4.3. AML Training
Speend.io ensures that all employees and stakeholders receive regular training on AML policies and procedures. This training helps maintain awareness and understanding of AML regulations and best practices.

The timing and content of the training provided is determined according to the needs of the Company. The frequency of the training can vary depending on to the amendments of legal and/or regulatory requirements, employees' duties as well as any other changes in the business model. The training program aims to educate the Company's employees on the latest developments in the prevention of money laundering and terrorist financing, including the practical methods and trends used for this purpose.

4.4. Record Keeping
Speend.io maintains comprehensive records of customer information, transactions, and AML-related documentation, no less than five years after termination of the business relationship.

The Company implements necessary rules for the protection of personal data upon application of the requirements arising from its obligations hereunder.

The Company may process personal data collected under this Policy only for purposes permitted by applicable law, including KYC/KYB, AML/CTF compliance, sanctions screening, fraud prevention, transaction monitoring, reporting to competent authorities, record keeping, compliance with legal obligations, and protection of the Company's rights and legitimate interests. Such data shall not be used for unrelated purposes unless permitted by applicable law or based on another valid legal ground.

5. REPORTING AND COMPLIANCE

5.1. Reporting Suspicious Activities
Where the Company identifies any activity, transaction, facts or circumstances that may indicate the use of proceeds of crime, money laundering, terrorist financing, sanctions evasion, fraud or any other unlawful activity, or an attempt to commit any of the foregoing, the Compliance Officer shall review and escalate such matter in accordance with the Company's internal AML/CTF procedures.

If, following internal review, the Company knows, suspects or has reasonable grounds to suspect that a transaction, customer, activity or circumstance may be connected with money laundering, terrorist financing, sanctions evasion, fraud or other criminal activity, the Compliance Officer shall ensure that the matter is reported to the competent authorities, where required under applicable laws and regulations.

The Company shall maintain internal records of suspicious activity reviews, decisions, supporting documents and reports submitted to competent authorities, where applicable.

5.2. Compliance Reviews

The Company conducts regular internal AML/CTF compliance reviews to assess the effectiveness of its AML/CTF framework, policies, procedures, internal controls, customer due diligence measures, sanctions screening, transaction monitoring and reporting processes. Based on the results of such reviews, the Company may update its policies, procedures, risk assessment methodology, monitoring rules, escalation processes and other internal controls to ensure continued compliance with applicable legal and regulatory requirements and recognized industry standards.

6. KYC / KYB Policy

Speend.io is committed to providing secure, transparent and reliable cryptocurrency processing and related services. Security, compliance and clarity in cooperation with our clients and partners are among our key priorities. To protect our platform, clients, partners and the integrity of our services, we apply KYC / KYB procedures before granting access to certain products and services. These procedures help us identify and verify our clients, understand their business activities, assess potential risks and comply with applicable AML/CTF, sanctions and other legal and regulatory requirements.

7. KYC/KYB PROVIDER

For certain KYC/KYB, AML screening and verification procedures, the Company may use third-party service providers, including AMLBot. Such providers assist the Company with identity verification, document checks, sanctions screening, risk assessment, transaction monitoring and related compliance processes.

AMLBot's verification platform is designed to support AML/CFT compliance processes based on a risk-based approach and recognized international standards, including the FATF Recommendations.

The Company remains responsible for determining the purposes and scope of processing in accordance with applicable laws and its internal policies. Third-party providers process data subject to applicable contractual, technical and organizational safeguards.

8. VERIFICATION TERMS

Documents verification may take up to 3 business days from the date of submission.

9. DATA PRIVACY

We strictly adhere to the principles of confidentiality, security and data protection.

All data provided to us will be processed securely and used only for purposes permitted by applicable law, including identity verification, KYC/KYB, AML/CTF compliance, sanctions screening, fraud prevention, transaction monitoring, reporting to competent authorities where required, record keeping, compliance with legal obligations, and protection of the Company's rights and legitimate interests.

Personal data may be shared with third-party service providers, compliance tools, banks, payment providers, crypto service providers, regulators, competent authorities or other relevant parties where

necessary for compliance, provision of services, risk management or legal purposes, subject to applicable laws and safeguards.

10. CONCLUSION

Speend.io is fully committed to combating money laundering and terrorist financing. Our AML Policy reflect our dedication to maintaining the highest standards of integrity and regulatory compliance in all our operations.

We continuously monitor and adapt our AML measures to evolving risks and regulatory changes to ensure the safety and security of our platform and users.

By adhering to this AML Policy, Speend.io aims to contribute to a safer and more transparent financial ecosystem while providing our customers with reliable and compliant cryptocurrency payment gateway services.

This AML Policy is subject to periodic review and updates to ensure its effectiveness and alignment with the latest AML and KYC regulations. Speend.io reserves the right to modify this policy as required, and any such changes will be communicated through our official website.

For any inquiries or reports related to AML and KYC/KYB compliance, please contact us: compliance@speend.io