FINZY

AML / CFT NOTICE

Information for Finzy Users

Finzy Sociedad de Responsabilidad Limitada
Legal entity No. 3-102-921514, Republic of Costa Rica
Version 1.0 | Effective date: 30 March 2026

Finzy complies with international anti-money laundering and countering the financing of terrorism (AML/CFT) standards established by the FATF and applies them to its products in the same manner as leading global cryptocurrency platforms. This page explains what this means for you as a User of the Service, why checks may be required, and how your actions affect the availability of the Service's features.

What AML/CFT Is and Why It Matters

Money laundering is the process by which criminals attempt to make proceeds of illegal activity, including fraud, corruption, illicit trade, or cybercrime, appear legitimate. Terrorist financing is the provision of funds or other financial support to terrorist organisations or individuals connected with terrorist activity.

Anti-money laundering and countering the financing of terrorism (AML/CFT) is a body of rules and procedures that financial institutions and virtual asset service providers (VASPs), including Finzy, apply to prevent their services from being used for unlawful purposes. These rules are an international standard applied by virtually all regulated cryptocurrency platforms worldwide.

Compliance with AML/CFT standards protects not only the financial system as a whole but also Users themselves, by reducing the risk of involvement in transactions connected with criminal activity, fraud, sanctions restrictions, or unreliable counterparties.

Identity Verification (KYC)

Know Your Customer (KYC) is the procedure by which the Company establishes and confirms a User's identity before granting access to certain features of the Service, in particular deposit, withdrawal and exchange operations.

As part of KYC, a User may be asked to provide an identity document, a photograph or biometric check for comparison against the document, residential address details, and, in certain cases, additional information or documents concerning the source of funds.

The scope of information requested depends on the risk level, nature, and volume of transactions. The higher the risk of the transaction or the User's profile, the more extensive the verification that may be required.

Confirmation of Source of Funds

In certain cases, the Company may request documents confirming the lawful origin of a User's funds or capital. This may be required, for example, during enhanced due diligence, where internal limits are exceeded, or where heightened risk factors are identified.

Such documents may include, among others, income statements, bank statements, documents relating to the sale of property, inheritance documents, or other materials enabling the source of funds to be established.

Transaction Monitoring

Finzy continuously monitors User transactions to detect indicators that may point to money laundering, fraud, terrorist financing, sanctions evasion, or other unlawful activity. Such monitoring may cover both transactions within the Service and virtual asset addresses from or to which funds are transferred.

Where heightened risk indicators are identified, a transaction may be temporarily suspended for additional review. Such a request or suspension does not by itself constitute an automatic finding of any violation.

Sanctions Screening and Geolocation Controls

The Company performs sanctions screening of Users and transactions, including checks against international sanctions lists and politically exposed persons (PEP) lists, both at registration and throughout the period of use of the Service.

To comply with restrictions on prohibited jurisdictions and sanctions requirements, Finzy may also use geolocation and technical control tools, including analysis of IP addresses and other technical data, both when accessing the account and when performing transactions.

Travel Rule

Transfers of virtual assets between platforms via Finzy may be subject to the requirements of the international standard known as the Travel Rule. In accordance with this standard, the Company may collect, store and transmit certain information about the sender and recipient of a transfer to the extent necessary to comply with applicable requirements.

If a transfer is directed to a platform, wallet, or address that does not allow applicable requirements to be met, the Company may request additional information or restrict the ability to make such a transfer.

Transfers to Non-Custodial Wallets

Where assets are transferred to a non-custodial (self-hosted, self-custody) wallet, or received from such a wallet, the Company may request additional information to confirm ownership of the address or the identity of the counterparty. Such measures are aimed at preventing circumvention of mandatory identification and control procedures.

What Happens If Suspicious Activity Is Detected

Where the Company reasonably concludes that a transaction or a User's activity may be connected with unlawful activity, the Company is entitled, and in required cases obliged, to file a corresponding report with the competent authority.

In cases provided for by law, the Company is not permitted to notify the User of the fact that such a report has been filed or of the content of its interaction with competent authorities.

Depending on the circumstances, the Company may request additional documents or explanations, temporarily suspend a transaction, restrict access to part of the account's functions or funds, or terminate servicing of the account in the manner provided for by the Terms of Service and applicable requirements.

Data Retention and Protection

Data collected as part of AML/CFT procedures is retained for the period necessary to comply with applicable legal requirements and the Company's internal procedures, generally not less than five years after termination of the relationship with the User, unless a longer period is required by applicable law or a lawful request of a competent authority.

The processing and protection of such data is carried out in accordance with the Finzy Privacy Policy and applicable information security measures.

User Obligations

By using Finzy, the User is obliged to provide accurate and up-to-date information, respond in a timely manner to the Company's requests for additional documents or explanations, refrain from using the Service on behalf of third parties without disclosing the relevant information, and refrain from conducting transactions connected with unlawful activity, sanctions evasion, or attempts to avoid verification.

Breach of these obligations may result in restriction or termination of access to the Service in the manner provided for by the Terms of Service and the Company's internal procedures.

Contact

If a User has questions about the reasons for additional verification or the status of their account, they may contact Finzy support at info@finzypay.io.

This information has been prepared for reference purposes for Users of the Service on the basis of international FATF standards and practices applied by leading global virtual asset platforms, and does not replace the Company's internal AML/CFT Policy.