AML Policy

Last updated: 23 October 2026

This Anti-Money Laundering and Counter-Terrorist Financing Policy ("AML Policy") describes the measures CrypTins applies to prevent the use of its services for money laundering, terrorist financing, sanctions evasion and other financial crime. It applies to all Merchants and all transactions processed through cryptins.com and the CrypTins merchant services.

1. Principles

- We work only with verified Merchants and do not open anonymous accounts.
- We apply a risk-based approach: the depth of checks depends on the risk of the Merchant, its business and its transactions.
- We comply with applicable AML/CTF laws and sanctions regimes and follow the recommendations of the Financial Action Task Force (FATF).
- We cooperate with competent authorities and report suspicious activity where required by law.

2. Compliance function

A designated compliance officer is responsible for this Policy, for reviewing alerts and escalated cases, and for reporting suspicious activity. Compliance questions can be sent to info@cryptins.com.

3. Merchant due diligence (KYC)

Every Merchant must complete identity verification in the account settings before accepting payments. Standard verification includes:

- a valid government-issued identity document;
- a selfie or liveness check matched against the document;
- information about the business, its website and the goods or services offered;
- screening against sanctions lists, politically exposed persons (PEP) lists and adverse media.

Where a Merchant acts for a company, we may also request company registration documents and information about directors and beneficial owners.

4. Enhanced due diligence

For higher-risk Merchants, such as those with high expected volumes, links to higher-risk countries, PEP status or unusual transaction patterns, we may require additional measures, including proof of address, information on source of funds and source of wealth, licences for regulated activities, and senior management approval of the relationship.

5. Ongoing monitoring

- Incoming payments and outgoing Payouts are screened using blockchain analytics for links to sanctioned entities, darknet markets, mixers, stolen funds and other high-risk sources.
- Transactions with an elevated risk score may be held until the review is completed.
- Merchant activity is compared with the information provided at onboarding, and unusual activity is investigated.
- Merchant information is reviewed periodically and when documents expire or the risk profile changes.

6. Holds, returns and reporting

Where a transaction requires review, we may hold the funds and request information from the Merchant. Depending on the outcome, funds may be credited, returned to the source address minus the network fee, or frozen and reported to the competent authority as required by law. We are not obliged to inform the Merchant about a report made to authorities where this is prohibited by law.

7. Travel Rule

Where required by applicable law, we collect and exchange information about the originator and beneficiary of transfers with other virtual asset service providers.

8. Prohibited businesses

We do not provide services to Merchants involved in:

- unlicensed gambling, betting or lotteries;
- mixers, tumblers and other services designed to hide the origin of funds;
- unlicensed money transmission, exchange, investment or lending services;
- pyramid, Ponzi or other fraudulent investment schemes;
- weapons, ammunition and explosives;
- narcotics and other controlled substances;
- adult content involving minors or non-consenting persons, and escort services;
- counterfeit goods and intellectual property infringement;
- terrorist financing, extremism or any activity subject to sanctions;
- any other activity that is illegal in the Merchant's or Customer's jurisdiction.

9. Restricted jurisdictions

We do not provide services to Merchants that are resident in, incorporated in or operating from countries and territories subject to comprehensive sanctions or identified by FATF as high-risk jurisdictions subject to a call for action, including: Cuba, Iran, North Korea, Myanmar, Syria, and the regions of Crimea, Donetsk, Luhansk, Kherson and Zaporizhzhia under occupation. We also do not

provide services to residents of the United States of America and its territories. The list is reviewed regularly and may be extended at our discretion or where required by law.

10. Record keeping

Verification data, transaction records and compliance decisions are kept for at least five years after the end of the business relationship, or longer where required by law.

11. Training

All staff with access to Merchant data or transactions receive AML/CTF training when they join and at least once a year.

12. Merchant obligations

Merchants must provide accurate information, respond to information requests within the requested time, use the services only for the declared business and inform us of any material change. Failure to do so may result in suspension or termination of the Merchant Account in accordance with the Terms of Service.

13. Review of this Policy

This Policy is reviewed at least once a year and whenever applicable laws or our services change. The current version is always available at cryptins.com.