DOCUMENTS

# AML/KYC policy

1 General provisions

This document describes how the ATOM service checks orders, transactions and addresses against AML/KYC requirements: which tools and risk thresholds apply, when verification is requested and what happens to an order flagged as high risk. The policy is part of the service rules published at atom-exchange.com.

## 1 General provisions

1.1 The ATOM service (atom-exchange.com) may request additional data from the User to verify their identity. If there are signs of fraud or invalid personal data, the order is rejected.

1.2 Checks are carried out both by the Service's own means and with the help of third-party services that check counterparties and addresses.

## 2 AML check tools

2.1 To assess risks, the Service uses AML analysers. The Risk Score is calculated from the analyser's data.

2.2 Thresholds: high-risk (High) transactions undergo a mandatory additional check; medium-risk (Medium) ones may be put on hold for verification; low-risk (Low) ones are processed as usual.

## 3 Risk Score model and transaction processing

3.1 The Service applies an automatic risk assessment system to incoming transactions and to the addresses it sends funds to, in order to prevent operations that violate AML requirements.

3.2 The Risk Score is made up of data from payment providers, third-party analytics systems and the Service's internal algorithms.

3.3 The check takes into account: risk labels of addresses and transactions; the history of fund movements and links with high-risk sources; behavioural signs (frequency, volume, structure of operations); data from external analytics services; other factors under the Service's AML policy.

3.4 The final Risk Score is expressed as a percentage from 0 to 100.

## 4 Thresholds and processing

4.1 0–49% — low risk. The order is fulfilled as usual.

4.2 50–79% — elevated risk. The order may be put on hold for an additional check. The User may be asked to confirm the source of funds, provide documents, prove ownership of the address and provide other information.

4.3 80% and above — high risk. The order is put on hold or rejected until the check is complete. It can be fulfilled only after successful verification or a decision based on the analysis.

## 5 High-risk labels

5.1 Certain label categories lead to a hold or rejection regardless of the final Risk Score. They include: sanctioned addresses; addresses linked to fraud; illegal services; financing of prohibited activities; darknet services; mixers and anonymising services; other high-risk categories under the classification of AML providers.

## 6 Additional check

6.1 In case of elevated or high risk, the Service may request an extended KYC check. The deadline for providing data is set individually and communicated on the order page

or by email.

6.2 If the User does not provide the data or it is not enough to complete the check, the order is closed in one of two ways: the funds are returned to the sender within a reasonable time (usually 7–10 business days) with confirmation of the refund, or the information is passed to the competent authorities if there are grounds for it.

6.3 Holding funds indefinitely without legal grounds and without an official escalation is not allowed.

6.4 The Service does not disclose the details and algorithms of the Risk Score model to prevent circumvention of control mechanisms.

## 7 Verification procedure (KYC)

7.1 Verification is required to receive payment details and takes place on the order page. The User selects the document type, uploads a photo of the document and a photo of their face and confirms the phone number from which the payment will be made.

7.2 To carry out anti-fraud checks and identity verification, the Service may share the User's data (full name, phone number, document details, photos of the document and face) with its specialised partner beorg.ru, which protects the data in accordance with Russian Federal Law No. 152-FZ.

7.3 Photo requirements: the document is fully visible, without glare, cropped edges or watermarks; all data is legible and not covered by anything; the face is shown from the front, without a hat or dark glasses, in sufficient light.

7.4 Accepted documents: Russian passport, foreign passport, ID card.

7.5 If verification fails, the User may go through it again. Payment details are not issued until verification is passed.

## 8 Recipient wallet check

8.1 After the payment is credited, the address where the User receives cryptocurrency undergoes an AML check under the rules of sections 3–5.

8.2 If the address fails the check, no payout is made, and the User is asked to specify another address on the order page. The User's funds are kept until a suitable address is specified, or are returned under the rules of section 9.

## 9 Refunds and holds

9.1 The Service does not hold funds indefinitely. Every order that is put on hold or rejected ends either with a refund or with an official escalation — always one of these two outcomes.

9.2 The refund is made to the sender within a reasonable time (7–10 business days) with transaction confirmation (TXID). The Service may withhold a processing fee of up to 5% of the amount, but no more than $100.

9.3 Refunds are available only to verified Users for whom no reasonable links to money laundering or other unlawful activity have been found.

9.4 Grounds for a refund or escalation: the User refuses to go through KYC; the data is not provided within the set deadline; high risk under AML/Risk Score; other situations where the order cannot be fulfilled.

## 10 Procedure for High Risk without confirmed unlawful activity

10.1 If a transaction receives the High Risk status in categories without confirmed unlawful activity, the Service carries out an internal analysis.

10.2 If no link with high-risk entities is confirmed, the order is not fulfilled, and the funds are returned only to the sender. No additional KYC is required for such a refund.

10.3 The refund period is 7–10 business days, taking into account network and payment infrastructure fees.

10.4 This procedure applies only if there are no signs of deliberate circumvention of compliance or other circumstances that require an extended check.