Policy

Account drainage detection

`account-drainage-aml-v1 - v1.0`

Effective: 2026-04-25
Owner: AML / Fraud investigations
Applies to: wire_transfer, cash_out

Purpose

This policy defines the AML rule for detecting and blocking the canonical "sweep and cash-out" fraud signature in real time, before the transaction is committed.

Detection rule

Account drainage attempts must be denied. An attempt is identified when all three of the following hold simultaneously:

- The transaction amount is at least 95% of the source account's pre-transaction balance (origin_balance_before)
- The transaction_type is TRANSFER or CASH_OUT
- The recipient's pre-transaction balance (recipient_balance_before) is below $100

Any single one of these signals on its own is not sufficient -- large transfers between established accounts are legitimate, and clearing out a balance occasionally is normal. The combination -- sweeping nearly the full balance into a near-empty recipient via a transfer or cash-out -- is the canonical "sweep and cash out" fraud signature.

Required action

When all three conditions trip:

- Decline the transaction with reason_code='account_drainage_aml'
- Flag the originating account (origin_account) for fraud investigation by emitting an incident record
- Do NOT route the request to manual review. This is a hard deny.

The drainage signature has near-zero false-positive rate when all three conditions are present together.

Why this rule exists

The Federal Reserve's payment-fraud studies and academic work (Lopez-Rojas et al. 2016 PaySim paper, FinCEN SAR analyses) identify this triple-condition pattern as the dominant signature in mobile-money and online-banking fraud. Catching it at the policy layer rather than at a downstream fraud-detection model gives the auditor a clear, citeable reason for the denial.