Anti-Money Laundering (AML) Compliance Policy

Global Financial Services Inc. — Version 3.0 — Effective February 2026

1. Purpose

This policy defines mandatory rules for detecting and preventing money laundering in the transactions database. The database contains fields: Timestamp, From Bank, From Account, To Bank, To Account, Amount Received, Receiving Currency, Amount Paid, Payment Currency, Payment Format, and Is Laundering flag.

2. Transaction Amount Rules

Rule 2.1: Large Transaction Reporting

Any transaction where Amount Paid exceeds 10,000 (in any currency) must be flagged for mandatory review. This is a regulatory requirement under AML laws.

Rule 2.2: Very High Value Transactions

Any transaction where Amount Paid exceeds 50,000 must be classified as critical severity and escalated immediately to the compliance team.

Rule 2.3: Round Amount Detection

Transactions where Amount Paid is a perfectly round number (divisible by 1000) and exceeds 5,000 must be flagged. Round amounts are a common laundering indicator.

Rule 2.4: Currency Mismatch

Any transaction where Payment Currency differs from Receiving Currency must be flagged for review. Cross-currency transactions require enhanced due diligence.

Rule 2.5: Amount Discrepancy

Any transaction where Amount Paid differs from Amount Received by more than 5% must be flagged. Significant discrepancies may indicate fee manipulation or layering.

3. Payment Format Rules

Rule 3.1: High-Risk Payment Formats

All transactions using Bitcoin or Cash as Payment Format must be flagged for enhanced monitoring. These formats are commonly used in money laundering.

Rule 3.2: Wire Transfer Threshold

Wire transfer transactions exceeding 5,000 in Amount Paid must undergo additional compliance review.

4. Account Behavior Rules

Rule 4.1: Self-Transfer Detection

Any transaction where From Account equals To Account (self-transfer) must be flagged as suspicious. Self-transfers are a known structuring technique.

Rule 4.2: Same Bank Large Transfers

Transactions where From Bank equals To Bank and Amount Paid exceeds 20,000 must be reviewed. Internal large transfers may indicate layering.

5. Known Laundering Flag

Rule 5.1: Flagged Transactions

Any transaction where the Is Laundering field equals 1 must be immediately escalated as a critical violation. This represents confirmed or suspected laundering activity identified by the detection system.

6. Severity Classification

Critical: Is Laundering = 1, or Amount Paid > 50,000
High: Amount Paid > 10,000, or Bitcoin/Cash payment format
Medium: Currency mismatch, round amounts, or self-transfers
Low: Wire transfers > 5,000, same-bank large transfers

7. Compliance

All flagged transactions must be logged, assigned severity, and reviewed within 48 hours. Failure to enforce these rules may result in regulatory penalties.

Approved by: Chief Compliance Officer — Review Date: February 2027