

# ANNEXURE A: INDICATIVE RED FLAGS CHECKLIST

## (For the Internal Use of the Risk Management System [RMS], Compliance, and Surveillance Teams)

The surveillance and risk management teams must monitor trading terminals, ledger systems, and demat accounts for the following red flags. Transactions matching these parameters must be escalated to the **Principal Officer** within **24 hours** for further investigation under the PMLA framework.

---

### 1. Client Onboarding & Verification Red Flags

- **Reluctance to Provide Info:** Client shows extreme reluctance to provide identity, address, or financial status proofs during onboarding.
- **Suspicious Credentials:** Documents submitted appear altered, blurred, newly counterfeited, or cannot be verified via automated digital KYC checks.
- **Unusual Location Mismatch:** Client's residential or business address is located in a geographic area known for high financial crime or drug-trafficking, with no logical link to their place of work.
- **PEP Non-Disclosure:** A Politically Exposed Person (PEP) or their close relative attempts to hide their political affiliation or background during onboarding.

### 2. Banking, Funding & Pay-In Red Flags

- **Third-Party Fund Attempts:** Frequent attempts to deposit trading funds from bank accounts or credit cards not registered under the client's name.
- **Multi-Account Splitting:** Funds arrive via small transfers from multiple, distinct bank accounts belonging to the same client without any economic rationale.
- **Cash-Equivalent Structuring:** Multiple cash deposits or demand drafts below ₹50,000 made directly into the broker's pool account at different bank branches.
- **Sudden Large Settlements:** Client suddenly clears a long-standing debit balance using a massive, unexpected fund transfer from an unknown or newly added bank account.

### 3. Trading & Portfolio Red Flags

- **Disproportionate Volume:** Trading volumes or contract values are completely disproportionate to the client's declared annual income or net worth.
- **Synchronized/Circular Trading:** Client appears to execute matching buy/sell orders synchronized with the exact timing and volume of another client (indicative of market manipulation or money movement).
- **Illiquid Scrip Concentration:** High-volume trading concentrated in low-volume, highly illiquid "penny stocks" or Z-group shares with no apparent market drivers.

- **Reversal Trades in Options:** Execution of paired options trades (buy and sell options of same strike and expiry) that result in a deliberate, manufactured loss for one party and gain for another.

#### 4. Demat & Off-Market Transaction Red Flags

- **Off-Market Asset Shifting:** High-value transfer of shares via delivery instruction slips (DIS) to third-party demat accounts categorized without valid reasons like "gift" or "inheritance."
- **Immediate Liquidation:** Large volumes of physical shares or off-market transfers received into a demat account, followed by immediate electronic sale and a request for an urgent cash payout.
- **U-Turn Movements:** Securities are transferred into a demat account off-market, immediately sold, and the funds are routed back out to a completely different banking channel.

#### 5. Account Maintenance & Operational Red Flags

- **Sudden Dormant Activation:** A trading account that lay dormant for over 12 months suddenly executes massive, high-value trades or receives large funds.
- **Frequent Profiling Updates:** Client frequently changes critical information like registered email IDs, mobile numbers, and bank account links within short intervals.
- **Anxious Payout Requests:** Client insists on immediate payout of funds while ignoring standard settlement cycles, or expresses unusual anxiety about regulatory reporting thresholds.

---

#### Internal Escalation Workflow for Flagged Alerts

[RMS Alert Triggered] -> [Preliminary Compliance Audit] -> [PO Evaluation within 48 Hours] -> [File STR or Log Internal Case]

1. **Log & Lock:** Once an alert is confirmed, the compliance team must archive the trade logs, ledger records, and communication history.
2. **The 7-Day Window:** If the Principal Officer deems the escalation suspicious, an **STR (Suspicious Transaction Report)** must be drafted and submitted via the FIU FINNET portal within **7 working days**.

