FAIR INTERMEDIATE INVESTMENT PVT. LTD.

Standard Operating Procedure (SOP) to manage surveillance alerts in broking and depository participant (DP) operations

This Standard Operating Procedure (SOP) is a structured framework developed by our company to manage surveillance alerts in broking and depository participant (DP) operations. It ensures compliance with regulatory bodies such as SEBI and depository (CDSL) guidelines to detect and mitigate market manipulation, money laundering, and fraudulent activities.

Purpose and Scope

Purpose: To define a workflow for creating, investigating, and resolving surveillance alerts to ensure market integrity.

Scope: Applies to all transactional and demographic alerts, whether generated internally or received from depositories (CDSLs) and exchanges.

Roles and Responsibilities

Role	Responsibility
Maker (Analyst)	Downloads alerts, conducts initial due diligence, collects client rationale, and proposes closure or escalation.
Checker (Manager)	Reviews the Maker's findings, validates supporting documents, and approves the disposal.
Compliance Officer	Oversees the entire process, reports "Adverse Observations" to regulators, and reviews the SOP annually.
Principal Officer	Final authority for filing Suspicious Transaction Reports (STR) with FIU-India.
IT support	Maintains and updates the monitoring system
Senior management	Oversees the effectiveness of the monitoring process.

Alert Generation Parameters

Alerts are generated based on predefined "themes." Key indicators include:

- **Demographic Alerts:** Multiple accounts with the same PAN, mobile number, or email; frequent changes in KYC details (address, bank, etc.).
- **Transactional Alerts:** High-value off-market transfers; transactions not commensurate with the client's declared income/net worth.
- **Behavioural Alerts:** A new account showing a sudden surge in volume followed by immediate dormancy; frequent "Gift" reason codes for transfers to unrelated parties.
- **Market Alerts:** Concentrated trading in illiquid or ASM/GSM (Additional/Graded Surveillance Measure) stocks.

Operational Workflow

Step 1: Alert generates & Triage

Frequency: Alerts from the depository are typically processed on a weekly/monthly basis. Internal alerts are reviewed daily (T+1).

Alert Generation: The monitoring system automatically creates alerts based on predefined rules and thresholds set by regulatory bodies and internal risk management teams

Step 2: Initial Analysis (Maker)

The Maker reviews the client's past trading/holding patterns. It is determined whether the client's transaction values match the income range and activity recorded in the account.

Step 3: Reason for request

If any activity appears suspicious, Maker contacts the client via registered email/phone, asking for the reason and supporting documents (e.g., bank statement, demat statement, income proof, KYC proof) if required. This is also updated in the database of all portals used by the company.

Detailed Analysis: Additional investigations are applied to high-risk alerts.

- Compliance may investigate further or request additional information
- Periodic reports are generated for review by senior management.
- Regular updates and improvements are made to alert parameters based on trends and regulatory changes.
- Periodic compliance audits and self-assessments.
- Emergency measures can be implemented in case of system failures or major security threats.

Exception Handling: Any deviations from the SOP should be documented and approved by senior management.

Verification & Disposition

- **False Positive:** If the explanation is valid and documented, the Maker marks it for closure with "Satisfactory Rationale."
- **Genuine Alert:** If the client fails to provide a rationale or the activity indicates manipulation, the Maker marks it as "Adverse."

Step 4: Maker-Checker Review

The checker reviews the case. If satisfied, they authorize closure. If more information is needed, the alert is returned to the maker for revision.

Timelines & Reporting

Regulatory compliance requires strict adherence to the following timelines:

Activity	Deadline
Review & Disposal	Within **30 days** of alert generation.
Adverse Observations	Report to Depository within **7 days** of identification.
STR Filing	As per PMLA guidelines (usually within 7 days of concluding suspicion).
MIS to Board	**Quarterly** (summary of pending, closed, and reported alerts).

Training and Awareness

Regular training sessions for staff involved in surveillance activities.
Awareness programs to keep staff informed about emerging risks and compliance updates

Compliance and Regulatory Requirements

Adherence to guidelines issued by regulatory bodies such as SEBI, RBI, and relevant exchanges

Record Keeping

All records, including client communications, bank statements, and internal notes, are maintained by our staff in easily accessible electronic or physical formats for a minimum period of 5 years (or as per current PMLA/SEBI requirements).

This SOP ensures a structured approach to DP surveillance, enhancing regulatory compliance and mitigating risks associated with fraudulent or suspicious transactions.

Policy created by: Kuldeep Trivedi

Policy reviewed by: Mansi Nagrath

Policy reviewed on: 05th Nov 2025

Policy approved by: Board of Directors Policy approved on: 05th Nov 2025