Standard Operating Procedure (SOP) for Processing Surveillance Alerts for Depository Participant

Objective

To define the standard procedure for managing and processing surveillance alerts, generated both at the Depository Participant (DP) end and by Depository, ensuring timely, effective, and secure handling of alerts.

Scope

This SOP applies to all surveillance alerts generated through Depository or internally by the DP. It establishes guidelines for alert generation parameters, response timelines, escalation procedures, and regular review requirements.

Roles and Responsibilities

Compliance Officer
Oversees SOP adherence, reviews alert parameters periodically, and ensures process improvement.

Alert Processor (Maker)
Identifies, reviews, and initiates the first level of alert handling.

Checker
Conducts secondary review to validate alert handling and ensures actions meet compliance standards.

Alert Generation Parameters

High-Value Transaction: Alerts for transactions exceeding a predefined threshold.
Transaction in Suspended ISIN: Transactions involving securities under suspension.
Simultaneous Changes in KYC and Demographic Details: When both KYC and personal details change in close proximity.
High-Value Transactions Post-Demographic Change: Large transactions following recent updates to account information.
Considerable Increase in Pledge Invocation: A significant rise in pledging securities within a short time.
Considerable Increase in Pledge: Substantial growth in securities pledged by the account holder.

Account Closed Shortly After Opening: Accounts closed soon after being established.
Off-Market Transfers Following Demographic Changes: Transfers post-changes in account information.
Off-Market Transfers Around Lock-In Period for Preferential Allottees: Transfers occurring during sensitive lock-in periods.
Multiple Demat Accounts with Common Contact Details: Multiple accounts linked by:

- - Mobile number
- - Bank details
- - PAN
- - Email address

Alert for multiple demat accounts opened with same demographic details: Alert for accounts opened with same PAN / mobile number / email id / bank account no. / address considering the existing demat accounts held with the DP.
Alert for communication (emails/letters) sent on registered Email id / address of clients are getting bounced.

Frequent changes in details of demat account such as, address, email id, mobile number, Authorized Signatory, POA holder etc.

Frequent Off-Market transfers by a client in a specified period.

Off-market transfers not commensurate with the income / Net worth of the client.

Pledge transactions not commensurate with the income / Net worth of the client.

Off-market transfers (High Value) immediately after modification of details in demat account.

Review of reasons of off-market transfers provided by client for off-market transfers vis-à-vis profile of the client e.g. transfers with reason code Gifts with consideration, frequent transfers with reason code Gifts/Donation to unrelated parties, frequent transfers with reason code off-market sales.

Alert for newly opened accounts wherein sudden increase in transaction activities in short span of time and suddenly holding in demat account becomes zero or account becomes dormant after some time.

Any other alerts and mechanism in order to prevent and detect any type of market manipulation activity carried out by their clients.

Procedures for Processing Alerts

Alert Identification: Alerts are automatically generated by Depository or DP's internal systems based on predefined parameters.
Initial Review (Maker): The Maker verifies alert details and assesses severity (low, medium, high).

Investigation and Response: Conduct an initial investigation, potentially contacting the relevant account holders for verification.
Final Review (Checker): Checker validates the actions taken by the Maker and confirms closure or escalation of the alert as necessary.

Escalation Procedure

Specific escalation paths depend on alert type and severity, with contacts for:

- - Immediate Supervisors
- - Compliance Officer

Time-lines for Response

Time-lines are as follows:

- - Initial review within 24 hours
- - Investigation and response within 3 business days
- - Final closure within 45 business days or sooner if required

Periodic Review

The Compliance Officer reviews the SOP and alert parameters quarterly to ensure compliance and operational effectiveness.

Maker-Checker Mechanism

The DP follows a Maker-Checker approach, with actions by the Maker validated by the Checker to ensure oversight and compliance.