Regulatory-Grade Manipulation Detection under Escalation

Stage 1 – Baseline Surveillance Validation

📅 28 February 2026 | 11:00 AM

1. Executive Context

The Surveillance Division has flagged suspicious trading activity across selected scrips and dates.

Potential mechanisms may include:

- Circular trading
- Reciprocal trading clusters
- Pump-and-dump coordination
- Infrastructure-linked coordination

Suspicion does not imply guilt.

You are appointed as the Independent Surveillance Analytics Advisory Team to:

- Validate suspected activity
- Refute false positives
- Classify mechanisms
- Expand detection beyond the suspect list

This is a regulatory-grade validation exercise.

2. Data Provided

You are provided:

- Orders file(s)
- Trades file(s)
- Suspicious list file(s) (by Scrip and Date)

The suspicious lists:

- May contain false positives
- May omit coordinated entities
- May include only partial clusters

Blind acceptance will be penalized.

📁 Orders File – Column Description

Column Name	Description	Data Type	Surveillance Relevance
Scrip Code	Unique identifier of the traded instrument	Nominal	Enables instrument-level segmentation and cluster analysis
ORDER_NUMBER	Unique identifier for each order	Nominal	Used to trace order lifecycle and match with trades
ORDER_DATE	Date on which order was placed	Date	Enables scrip-date slice analysis
Order Time	Timestamp of order entry (high resolution)	Timestamp	Critical for sequencing, synchronization, and front-running detection
Member Code	Broker identifier placing the order	Nominal	Used to detect broker-level concentration and routing patterns
Client Code	Unique client identifier	Nominal	Core unit for manipulation network analysis
Order Quantity	Quantity requested in the order (may be zero for modification/cancellation)	Numeric	Helps detect spoofing, layering, and abnormal size behavior
Value	Monetary value of the order	Numeric	Used to assess economic materiality and price-pressure intent
Order Type	Category of order (e.g., Limit, Market, Cancel, Modify)	Nominal	Critical for detecting cancellation patterns and order lifecycle anomalies
Terminal No	Trading terminal identifier	Nominal	Used to detect infrastructure concentration or shared access
Buy/Sell Flag	Indicates Buy (B) or Sell (S) side	Nominal	Required for directional sequencing and loop detection
Location Id	Geographic or exchange location identifier	Nominal	Used to detect shared infrastructure and cross-location coordination

Orders reflect **intent and pre-trade behavior**.

📁 Trades File – Column Description

Column Name	Description	Data Type	Surveillance Relevance
TRADE_NUMBER	Unique identifier for each executed trade	Nominal	Used to uniquely track execution events
TRADE_TIME	Timestamp of trade execution	Timestamp	Enables high-resolution sequencing and synchronization analysis
TRADE_DATE	Trade execution date	Date	Used for scrip-date slice segmentation
SCRIP_CODE	Instrument identifier	Nominal	Used for instrument-level network construction
BUY_MEMBER_CODE	Broker on buy side	Nominal	Used for broker-level clustering and routing patterns
SELL_MEMBER_CODE	Broker on sell side	Nominal	Used for broker-level clustering and routing patterns
Buy Client Code	Client on buy side	Nominal	Primary node for client-to-client network graph
Sell Client Code	Client on sell side	Nominal	Primary node for client-to-client network graph
BUY_TRADER_ID	Trader ID on buy side (if available)	Nominal	Used to detect shared infrastructure coordination
SELL_TRADER_ID	Trader ID on sell side (if available)	Nominal	Used to detect shared infrastructure coordination
TRADE_QUANTITY	Executed quantity	Numeric	Used to measure loop concentration and volume asymmetry
TRADE_RATE	Executed price per unit	Numeric	Used to detect price impact and pump patterns
TRADE_VALUE	Executed monetary value	Numeric	Used to assess economic significance of clusters
BUY_LOCATION_ID	Location of buy-side execution	Nominal	Used for infrastructure linkage analysis
SELL_LOCATION_ID	Location of sell-side execution	Nominal	Used for infrastructure linkage analysis
BUY_TIMESTAMP	Timestamp of buy-side order submission	Timestamp	Used to detect order-to-trade latency and front-running
SELL_TIMESTAMP	Timestamp of sell-side order submission	Timestamp	Used to detect order-to-trade latency and front-running

Trades reflect **realized counterparty interaction**.

3. Stage 1 Analytical Mandate

You must:

1. Validate suspected entities

Determine whether microstructure evidence supports manipulation.

2. Classify mechanism

Each entity or cluster must be classified as:

- Circular Trading
- Pump & Dump Coordination
- Infrastructure-Linked Coordination (if supported)
- Legitimate High-Activity Behavior
- Insufficient Evidence

3. Conduct network analysis

At minimum:

- Client ↔ Client trade graph
- Member ↔ Client linkage
- Reciprocity analysis
- Loop detection
- Synchronization patterns

4. Develop explainable risk scoring

Produce:

- Client-level risk score
- Member-level risk score
- Evidence strength index

5. Identify additional high-risk entities

Using:

- Network expansion
- Motif participation
- Synchrony similarity
- Counterparty concentration