

## **Consultation paper on institutional mechanism for Stock Brokers to ensure prevention and detection of fraud or market abuse**

### **1. Objective**

- 1.1. Preventing/ detecting fraud or market abuse is a key pillar of investor protection. Brokers are uniquely positioned to detect/ prevent market misconduct by their employees, associates, and clients.
  
- 1.2. This consultation paper solicits comments/ views from market participants on a proposal which requires broking firms and their senior management to be accountable for such detection/ prevention of fraud or market abuse, by setting up robust surveillance and control systems, and ensuring appropriate escalation and reporting mechanisms. This proposal also enumerates some of the common examples of market abuses that brokers must look to detect/ prevent, the entities who should be subject to surveillance, and the accountability that is entailed.

### **2. Background**

- 2.1. Brokers play a pivotal role in protecting the interest of investors and in developing securities markets. SEBI (Stock Brokers) Regulations, 1992 ("Broker Regulations") place broad responsibility on brokers to exercise due diligence by prescribing a code of conduct, and cast a responsibility on their compliance officer to monitor legal/ regulatory compliance.
  
- 2.2. A committee on Fair Market Conduct (hereinafter referred to as "Committee") was constituted in 2017 to address the issues related to market manipulation and fraud, insider trading, code of conduct related to insider trading and surveillance, investigation and enforcement process.
  
- 2.3. Based on recommendations of the Committee, SEBI (Prohibition of Fraudulent and Unfair Trade Practices Relating to Securities Market)

Regulations, 2003 ("PFUTP Regulations") and SEBI (Prohibition of Insider Trading) Regulations, 2015 ("PIT Regulations") were partly amended w.e.f. February 01, 2019.

2.4. The Committee also recommended that intermediaries should have a mechanism to prevent fraud or market abuse by clients and/ or their promoters/ directors/ Key Managerial Personnel (KMPs)/ employees/ authorised persons.

### **3. Need for institutional mechanism for Brokers**

3.1. Currently, there are no specific regulatory provisions requirements that cast responsibility on brokers to put in place systems for detection and prevention of fraud or market abuse.

3.2. The list of probable instances / indicators of fraud or market abuse which the broker's system should be equipped to monitor, at a minimum, are as follows:

- a) creation of misleading appearance of trading,
- b) price manipulation,
- c) front running,
- d) insider trading,
- e) mis-selling,
- f) unauthorized trading, including facilitation of 'mule' accounts that act as a front for unauthorized trading
- g) pump and dump,
- h) spoofing,
- i) disproportionate trading activity vis-à-vis reported income/net worth,
- j) frequent changes in KYC submitted by clients.

3.3. Instances of fraud or market abuse distort transparency, imperil market integrity and undermine the confidence of investors in the capital market.

Hence, there is a need for an institutional mechanism for brokers to ensure that systems are in place for detection and prevention of fraud or market abuse.

#### **4. Consultation with Market Participants**

The enclosed proposal was deliberated in a meeting of the Intermediary Advisory Committee (IAC) held on December 15, 2022, comprising, brokers, exchanges, market experts, and other stakeholders. Taking into account the recommendations of the IAC, it is proposed that an institutional mechanism for brokers to ensure detection and prevention of fraud or market abuse, may be prescribed by way of amendment to the Broker Regulations and/or through appropriate Circulars/ Guidance Notes.

#### **5. Proposed Regulatory Framework**

The following framework is proposed:

##### **A. Broker Senior Management Oversight over Surveillance**

- i. The CEO, MD, Compliance Officer, Principal Officer, KMPs, Directors or analogous persons of the broker ("senior management") shall be responsible to ensure robust, independent trade surveillance systems and internal control systems to ensure compliance with the regulatory requirements as may be prescribed by SEBI/ stock exchanges from time to time, to detect/ prevent/ report fraud or market abuse by its clients, promoters, employees (including senior management), Authorised persons (APs), or analogous persons. They shall be held accountable for non-compliance and negligence in implementing appropriate surveillance and internal control systems.
- ii. The Audit Committee and Board of broker, or such other analogous bodies of the broker, shall review compliance with the provisions of this framework

at least once a quarter and shall verify that the systems for internal control and reporting are adequate and are operating effectively.

#### **B. Setting up of robust surveillance systems**

- i. The broker shall have in place robust trade surveillance systems and internal control procedures that are commensurate with the nature of business and the size of its operations, to detect potential fraud or market abuse by its clients, promoters, employees (including senior management), APs, directors, or analogous persons. Standard Operating Procedures (SOPs) shall clearly document trade surveillance policies and procedures, roles and responsibilities and guidelines on the corrective action to be taken.
- ii. The board or equivalent of the broker shall review and update the systems, processes, and control procedures on a regular basis (at least once a year) to keep pace with market developments and regulatory changes including adoption of automated trade surveillance systems to enhance the monitoring of trading activities.
- iii. Broker shall have appropriate systems in place to ensure that their proprietary accounts are used only for the purpose of carrying on proprietary trades which are in line with the various regulatory requirements as have been laid down by SEBI/Stock Exchanges from time to time. There shall be no 'lending' of any proprietary accounts for facilitation of any unauthorised trading.
- iv. The broker shall customize their trade surveillance systems and internal controls in a manner which is commensurate with the complexity of cases in question as well as its business activities. The thresholds for alerts for various scenarios should be set at a reasonable level and should be documented with clear rationale.

### **C. Escalation and reporting mechanism**

- i. The broker shall have in place well-defined processes that detect potential fraud or suspicious trading activities that need to be escalated. The escalation processes should be properly documented and appropriately implemented so as to keep independent senior management informed of any instances of potential fraud or suspicious trading activities.
- ii. If the broker detects suspicious trading activities or trading patterns of concern, such findings shall be promptly informed to stock exchanges through the channels, as may be specified from time to time.
- iii. Brokers shall submit a summary analysis and action taken report on instances of suspected fraud or market abuse on a half-yearly basis to stock exchanges.
- iv. Any deviations along with proposed corrective action in adherence to internal controls, risk management policy, trade surveillance policy, client on boarding, unusual activity done by clients and PMLA policy shall be placed before appropriate Committee/ Board at regular intervals. Such deviations shall also form a part of the report to be submitted by the broker to the stock exchanges in terms of para (iii) above.
- v. Broker shall also engage with the stock exchanges in case it needs guidance on trade surveillance observations, such as trading activities which were repeatedly flagged but no conclusion could be made due to the limited information available with the broker.

### **D. Whistle blower policy**

- i. The broker shall establish, implement and maintain a well-documented policy that sets out the availability of whistle blowing channels, process for raising concerns about suspected fraudulent, unfair or unethical practices, violations of regulatory or legal requirements, governance weaknesses etc. by stakeholders including employees without any fear of punishment or

unfair treatment and procedures to ensure adequate protection of whistle blowers, and the procedures to handle whistle blowing complaints.

- ii. Such whistle blowing complaints may be addressed to audit committee (in case of listed entities) or analogous body (in case of complaint against Board of Directors including those against MD / CEO / KMPs /Directors/ Promoters) or Compliance Officer (in case of other complaints).

## **6. Proposed Guidance Note for detecting and preventing fraud or market abuse**

This guidance note is divided into three parts and is to be read in conjunction with the PFUTP Regulations, 2003, PIT Regulations, 2015, various circulars issued by SEBI and the Stock Exchanges from time to time, particularly with regard to trade surveillance:

1. *Indicative list of some of most common market abuse practices along with factors to be considered when assessing such practices;*
2. *Indicative list of entities who should be surveilled, controls for monitoring, and risks arising out of potential fraud or market abuse covered;*
3. *Accountability matrix.*

The scenarios and factors identified below are neither exhaustive nor definitive, and their monitoring and investigation processes should be tailored to be commensurate with the complexity of each case.

### **Indicative list of some of most common market abuse practices along with factors to be considered when assessing such practices<sup>1</sup>**

Some of the factors which should be considered when assessing suspicious trading activities for potential fraud or market abuse are listed below.

---

<sup>1</sup> Reference: Trade Surveillance Practice Guide of Monetary Authority of Singapore

<https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/MAS-SEX-Trade-Surveillance-Practice-Guide.pdf>

Type of activity	Factors to be assessed
<p><b>Creation of misleading appearance of trading:</b> Trading of a security that occurs at specified prices, volumes and time in a manner agreed upon by the market participants in an attempt to match each other's trades. It may involve a group of clients and/or APs acting in concert. Such trading behaviour has the effect of creating a false or misleading appearance of active trading in the security.</p>	<ul style="list-style-type: none"> <li>• Potential connections and relations between clients, based on KYC</li> <li>• Frequency of occurrence and quantity of matched trades that suggest pre-arranged, wash, or circular trading</li> <li>• Market impact, trades of disproportionate volumes</li> <li>• Time proximity of order entries</li> </ul>
<p><b>Price manipulation :</b> Trades that have the effect of artificially raising or lowering the market price of a security may create a false market. Such trades which cause significant price movements warrant greater scrutiny on the broker's part.</p>	<ul style="list-style-type: none"> <li>• Unusual price movements</li> <li>• Timing of trades near sensitive periods, such as end of month, quarter, before announcements</li> <li>• Timing of orders concentrated within a short time which causes price movement</li> <li>• Trades causing significant price movements</li> </ul>
<p><b>Front running :</b> Trade practice undertaken by a person in possession (directly or indirectly) of non-public information regarding a substantial impending transaction. Normally, this would apply to a person who trades while being privy to a Big Client Order.</p>	<ul style="list-style-type: none"> <li>• Time proximity of front running order and big client's order</li> <li>• Same or better price of front running order</li> <li>• Frequency and repeated patterns of occurrence</li> </ul>
<p><b>Insider trading :</b> Trading in securities that are listed or proposed to be listed on a stock exchange when in possession of unpublished price sensitive information.</p>	<ul style="list-style-type: none"> <li>• Market fluctuations around a material announcement</li> <li>• Change in trading behavior of clients and / or huge gains around a material announcement</li> <li>• Client's connections with the listed company as available from data with brokerage</li> </ul>
<p><b>Spoofing :</b> A person submits a large (non-bonafide orders) but not marketable limit order that raises the bid price of a security (or depresses the offer price of a security in</p>	<ul style="list-style-type: none"> <li>• Frequent cancellation or cancellation of large number of orders</li> </ul>

case of a large sell order) and/or greatly increases the quoted size at or around the current best bid price (best offer price in case of non bonafide sell order).

The large order causes market participants to match or better the price of the order. The person then cancels the large order and enters (virtually at the same time or just before the cancellation of the large non-bonafide orders), a sell order (buy order in case of non-bonafide large sell order) that matches the buy order of other investors at a higher price (sell order of other investors at a lower price).

- Placement of large orders above or below the prevailing price

**Indicative list of entities who should be surveilled, controls for monitoring, and risks arising out of potential fraud or market abuse covered are as follows:**

<b>Entity being surveilled</b>	<b>Controls for monitoring</b>	<b>Risks arising out of potential fraud or market abuse covered</b>
<b>Client</b>	Trade Surveillance alerts to trace matched trade, volume creation, penny scrip, unusual price movements, frequent cancellation or cancellation of large number of orders etc.	<ul style="list-style-type: none"> <li>• Creation of misleading appearing of trading</li> <li>• Front running</li> <li>• Unauthorised trading</li> <li>• Insider trading</li> <li>• Spoofing</li> <li>• Price Manipulation</li> <li>• Disproportionate trading activity vis-à-vis reported income/net worth</li> <li>• Sudden surge in Dormant account</li> </ul>
	Pre-trade controls like blocking of scrips based on surveillance assessment/illiquid contracts, additional margins in volatile scrips/contracts, trade execution range, etc.	
	Online alert/Nudge on the trading screen to warn the client before dealing in certain stocks like penny stocks, etc.	



		<ul style="list-style-type: none"> <li>Monitoring of sudden surge in client trading activity</li> <li>Activity in SMS stocks</li> <li>Client concentration in particular scrip</li> </ul>
	IP address Identification of multiple client codes trading from the same location	Mule accounts that attempt to conceal malpractices
	Calling to clients on sample basis based on broker's internally defined scenarios	Unauthorised trading or mis-selling
	Email and SMS alert on old contact details on change in email id / mobile of retail clients	<ul style="list-style-type: none"> <li>Frequent changes in KYC details/ account opening details</li> <li>Fraudulent contact details updation</li> <li>Fraudulent Account opening</li> </ul>
	Internal alert for same name/DOB with Multiple PAN	
Internal Alert for same bank account mapped to multiple clients. Controls during account opening to scrub against existing bank details.		
<b>Employees</b>	Listening to dealer calls (voice surveillance)	<ul style="list-style-type: none"> <li>Unauthorized trading</li> <li>Password Sharing</li> <li>Front running</li> <li>Insider Trading</li> <li>Fraud</li> <li>Data misuse</li> </ul>
	Email surveillance, coverage to be based on internal policy of members	
	Surprise visit of dealing rooms	
	Access to trading floor should be access controlled and subject to approvals by designated approvers	
	IP analysis to track internal IPs for self trading client	
	Restriction on mobile and smart watch in dealing room.	
	Having suitable internet access policies to restrict social networking sites on office network except for legitimate reasons like official marketing/promotion and to protect data upload on third party websites	

	Insider Trading policy - Verification of trade with pre-approval, periodic training to employees	
	Reporting of employee misconduct/frauds to senior management/committee	
	Access to drives/folders having Unpublished Price Sensitive Information (UPSI) restricted to relevant employees only	
	Access control mechanism by giving access to client data on a need to know basis	
	Background screening checks at the time of hiring	
	Whistle blower policy to report any fraudulent activity	<ul style="list-style-type: none"> <li>• Internal fraud or wrongdoing</li> </ul>
	Monitoring email sent outside organisation for senior employees	<ul style="list-style-type: none"> <li>• Data protection or any wrongdoing</li> </ul>
<b>Authorised Persons (AP)</b>	Surprise visit at AP office posing as a client at AP's office	<ul style="list-style-type: none"> <li>• Unauthorized trading</li> <li>• Fraudulent trading activity</li> </ul>
	Social Media Monitoring to check if APs are misusing broker's logo or promising any assured return	<ul style="list-style-type: none"> <li>• Offering assured returns</li> </ul>
	Recorded call verification on sample basis	<ul style="list-style-type: none"> <li>• Unauthorized use of terminal</li> </ul>
	Scrip level analysis of AP to check if AP is concentrating in any particular scrip	
	AP screening against negative databases	
	Calls to clients mapped to APs on sample basis	
<b>CEO / MD / KMPs</b>	Whistle blower policy to report any fraudulent activity.	Internal fraud or wrongdoing
	Monitoring email sent outside organisation for senior employees	Data protection or any wrongdoing
<b>Promoters</b>	Whistle blower policy to report any fraudulent activity.	Internal fraud or wrongdoing

### Accountability matrix

In addition to the above, the broker shall have an accountability grid for different types of suspicious behaviour. A model accountability grid is as under:

Who is being surveilled	Responsibility of trade surveillance on
CEO / MD/ Directors/KMPs	Board of Directors / Audit Committee (in case of listed entities)
Promoters	Board of Directors / Audit Committee (in case of listed entities)
Employees	CEO / MD/ Directors/KMPs
Clients	Official(s) responsible for trade surveillance under supervision of senior management
Authorised Persons	Official(s) responsible for trade surveillance under supervision of senior management

### 7. Public Comments

Considering the implications of the said matter on the market participants, public comments are invited on the above proposals. The comments/ suggestions may be provided as per the format given below:

Details of respondent				
Name of the person/entity				
Contact details				
Category	Whether market intermediary/ participant (mention type/ category) or public (investor, academican etc.)			
Sr. No.	Extract from Consultation Paper	Issues (with page/para nos., if applicable)	Suggestions	Rationale

Comments as per the above format mentioning the subject line as "Comments on Consultation paper on Institutional mechanism for Stock Brokers to ensure prevention and detection of fraud or market abuse" may be sent latest by February 21, 2023, through the following modes:

(i) preferably by email to Ms. Aradhana Verma at [aradhanad@sebi.gov.in](mailto:aradhanad@sebi.gov.in) and / or to Shri Gaurav Kumar at [gauravk@sebi.gov.in](mailto:gauravk@sebi.gov.in)

(ii) By post to the following address:

Ms. Aradhana Verma  
Deputy General Manager,  
Market Intermediaries Regulation and Supervision Department  
Securities and Exchange Board of India,  
SEBI Bhavan II, Plot No. C/7, G Block,  
Bandra Kurla Complex, Bandra (East),  
Mumbai - 400 051

Issued on: February 07, 2023