

**9-2/2021/Intermediaries/ FIU-IND
Government of India
Ministry of Finance
Department of Revenue
Financial Intelligence Unit-India.**

7th Floor, Tower-2
Jeevan Bharti Building,
Connaught Place,
New Delhi- 110001.

Dated: **31st** December, 2024

To,

The Designated Director & Principal officers of all Depository Participants

Subject: Guidelines for detecting suspicious transactions under rule 7(3) of Prevention of Money Laundering (Maintenance of Records) Rules, 2005-reg

For the purpose of reviewing the 'Red Flag Indicators (RFIs)' for Stock Brokers, Exchanges, Depositories and Depository Participants (DPs), a 'Working Group' was constituted consisting of members from the various stakeholder in the securities market including member from SEBI. The abovementioned working group recommended certain Red Flag Indicators (RFIs) for generation of alerts and for detecting Suspicious Transaction for Stock Brokers, Exchanges, Depositories and Depository Participants (DPs). FIU-India, on the basis of the recommendations of the working group, issued 'Supplemental Guidelines for Detecting Suspicious Transaction for Stock Brokers and Depository Participants (DPs)' vide communication dated 21/07/2022. Further, it was also mentioned in the aforesaid communication that these RFIs were in addition to the RFIs issued by FIU-India vide communication dated 11/03/2016 vide F.No.9-6/AG-II/2012/FIU-IND. With a view to ensure that **Depository Participants (DPs)** play more proactive role to safeguard the Indian financial system through strict, effective, and meaningful compliance with the obligations under the PMLA framework, it has been decided to issue a **Consolidated RFI Guidelines for generation of alerts and for detecting Suspicious Transactions by Depository Participants (DPs)**.

2. Sub-rule (3) of Rule 7 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005, as amended, empowers Director, FIU-IND to issue guidelines in consultation with Regulator for detecting suspicious transactions. These guidelines are being issued under the said Rule.
3. The RFIs which are proposed to be implemented by **Depository Participants (DPs)**, are mentioned in **Annexure-1**, which is enclosed herewith.
4. The alerts generated by using the RFIs as given in the guidelines should be properly analysed with a view to identify suspicious transactions as defined under the PML Rules, and if an RE comes to the conclusion that a case appears to be a suspicious transaction, then the case may be brought to the notice of FIU-IND by filing Suspicious Transaction Reports (STRs) following the prescribed procedure in this regard.



5. It may be mentioned that these RFIs are issued to facilitate the REs to generate alerts for detecting suspicious transactions. The thresholds prescribed in these RFIs are indicative. However, REs are free to adopt stricter criteria and lower thresholds, but REs may not adopt criteria less strict than that which is provided by FIU-IND herein in order to mitigate AML/CFT risks specifically in cases where purposeful avoidance of such thresholds are observed by the REs.

6. It should be noted that the process and analysis of the alerts should be carried out by the RE within its AML/CFT organizational setup in a manner that it should not lead to tipping-off. In this regard, REs are cautioned that the requirement of confidentiality regarding reporting of transactions to FIU-IND extends not only to the customers concerned but also to other REs. While sharing alerts with other REs or otherwise, care must be taken to ensure that the fact of whether an STR has been filed in relation to a specific transaction or alert is not directly or indirectly disclosed. Any deviation in this regard will be viewed strictly.

7. All the Designated Directors and Principal Officers of the REs concerned are requested to implement the guidelines with immediate effect and ensure their compliance.

8. Further, penalties for non-compliance with obligation under Chapter IV of PMLA (including obligations to report STRs and to have in place an effective mechanism to detect and report STRs) may range up to Rs. 1 Lakh per non-compliance.

Warning: This document is confidential and is intended for use only by the Designated Director, Principal Officer and the AML/CFT teams. Any circulation of this document to any other person is strictly prohibited. The REs are advised to ensure strict confidentiality of this document.

Yours faithfully,



(Vivek Aggarwal)
Director, FIU-IND

Enclosure: Annexure A - Consolidated RFI Guidelines for generation of alerts and for detecting Suspicious Transactions by Depository Participants (DPs). -reg

Copy to:

**Ms. Madhabi Puri Buch, Chairperson
Securities and Exchange Board of India
SEBI Bhavan, Plot No. C-4A
"G" Block, Bandra Kurla Complex
Bandra (East), Mumbai – 400 051**



(Vivek Aggarwal)
Director, FIU-IND

Annexure - 1: Consolidated Red Flag Indicators (RFIs) for detecting suspicious transaction by the Depository Participants (DPs) - Reg.

Alert Source	Alert Indicator	Indicative Rule/Scenario
Customer verification	CV1 - Customer left without opening account	Customer did not open account after being informed about KYC requirements
	CV2 - Customer offered false or forged identification documents	Customer gives false identification documents or documents that appear to be counterfeited, altered or inaccurate
	CV3 - Address found to be wrong	Customer not staying at address provided during account opening
	CV4 - Difficult to identify beneficial owner	Customer uses complex legal structures or where it is difficult to identify the beneficial owner
Law Enforcement Agency Query	LQ1 - Customer is being investigated for criminal offences	Customer has been the subject or inquiry from any law enforcement agency relating to criminal offences
	LQ2 - Customer is being investigated for TF offences	Customer has been the subject of inquiry from any law enforcement agency relating to TF or terrorist activities
	LQ3 - SEBI has passed orders under the SEBI Act, 1992 with Rules and Regulations made thereunder.	Customer's name appears in any Order passed by SEBI. SEBI has initiated an investigation and has restrained individuals/entities from buying, selling or dealing in the securities markets, either directly or indirectly, in any matter.
Media Reports	MR1 - Adverse media report about criminal activities of customer	Match of customer details with persons reported in media / open source for criminal offences.
	MR2 - Adverse media report about TF or terrorist activities of customer	Match of customer details with persons reported in media / open source for terrorism or terrorist financing related activities.
Employee Initiated	EI1- Customer did not complete transaction	Customer did not complete transaction after queries such source of funds etc.
	EI2- Customer provides inconsistent information	<ul style="list-style-type: none"> • Customer changes the information provided after more detailed information is requested. • Customer provides information that seems minimal, possibly false or inconsistent.



Employee Initiated	EI3 - Customer wants to avoid reporting	Customer makes inquiries or tries to convince staff to avoid reporting.
	EI4 - Customer could not explain source of funds	Customer could not explain source of funds satisfactorily
	EI5 - Transaction is unnecessarily complex	Transaction is unnecessarily complex for its stated purpose.
	EI6 - Transaction has no economic rationale	The amounts or frequency or the stated reason of the transaction does not make sense for the particular customer.
	EI7 - Transaction inconsistent with business	Transaction seems inconsistent with the customer's business.
	EI8 - Power of Attorney Transactions	Where orders are being placed by an individual who holds a POA but is not a family member.
	EI9 - Suspicious Closure of Account	1. Accounts closed within 30 days of opening of Account and single or series of debit transactions (On Market, Off-market including IDT Transfer) with value > Rs 10 lacs AND; Exclude own account transfer (first holder PAN) i.e., transfers made through account transfer cum closure module and with reason code transfer to own accounts. Also, if securities received in source account through transmission, then the same will be excluded
Public Complaint	PC1-Complaint received from public	Complaint received from public for abuse of account for committing fraud etc.
Business Associates	BA1 - Alert raised by agent	Alert raised by agents about suspicion
	BA2 - Alert raised by other institution	Alert raised by other institutions, subsidiaries or business associates including cross-border referral
Typology	TY1-Transactions similar to typologies found in Orders passed under the SEBI Act	Transaction pattern same as that in orders passed by SEBI under the SEBI Act.



Transaction Monitoring	TM1 - High value Deals - Single transaction	Single transaction of client is greater than INR(X) / quantities (Y) in a day/month/settlement. The specified amount may be compared with financial capability of the client as given in his KYC/Updated financials.
	TM 2 - High value Deals - Aggregate transaction	Aggregate transaction of Client is greater than INR(X1) / quantities (Y1) in a day/month or X% of average. Validate above transactions of client with his financial capability as per KYC/Updated financials.
	TM3 - Synchronized, Cross and Self Trades	Identify clients/group of clients who have undertaken off market/ market transactions on similar quantity of same shares either during a day or over a period of (x) days which seems suspicious.
	TM 4 - Turnover vis-à-vis financial income submitted by the client	<ul style="list-style-type: none"> • Identify clients whose turnover/ transaction is disproportionate with the annual income/ Net worth provided in KYC/Updated financials. • Scrutinize the transaction of such clients and follow up with concerned branches for collection of latest financials. <p>Separate benchmark to be applied for Income/ Networth and type of volume like off market/ market transaction etc.</p>
	TM 5 - High value transactions in a new account	<ul style="list-style-type: none"> • Transactions greater than INR(X2) /quantities (Y2) in newly opened account within [x1] days/months of account opening. The specified amount may be compared with the financial capability of the client as given in his KYC
	TM 6 - High value transactions in a dormant account	<ul style="list-style-type: none"> • Transactions greater than INR(X3) /quantities (Y3) in dormant account within [x2] days of reactivation
	TM 7 - Frequent Small quantity transactions in an account	<ul style="list-style-type: none"> • Transactions in small quantity aggregating to X % of total turnover of the client within the last (x3) days.
	TM 8 - Transaction in illiquid scrips/ unlisted scrips	<ul style="list-style-type: none"> • Market transactions in illiquid scrips/ unlisted scrips in small quantities within [x4] days which seems suspicious.



	<p>TM 9 – Off Market transfer to unrelated accounts</p>	<p>1. Only for Reason code/s -off-market sale -Gift -Donation AND;</p> <p>2. Valuation per debit transaction will be > 25 lacs AND;</p> <p>3. Exclude accounts with same PAN, mobile, email ID, same bank details (IFSC + ac no) (same mobile / email / bank details in multiple demat accounts) and family flag is enabled AND;</p> <p>4. valuation is > 5 times of income range</p>
	<p>TM 9A – Suspicious Off Market Credit and Debit</p>	<p>1. Customer receive credit / demat of 50,000 shares or shares worth Rs. 25 lakhs and above by single transaction or series of transactions in an ISIN AND;</p> <p>2. 80% or more of credited shares gets debited by way Off Market transfer to 3 or more than 3 unrelated accounts AND;</p> <p>Only Listed Equity Shares will be considered for this alert. (Monthly frequency) short span of time is within 30 days.</p>
	<p>TM 9B – Off market delivery in unlisted scrip</p>	<p>1. Single or Series of Transactions where more than 5,00,000 unlisted equity shares have been transferred within period of 1 month AND;</p> <p>2. Off-Market Transfers with Reason Code “Off-Market Sale”, “Donation “and “Gift” will be considered AND;</p> <p>3. Exclude own account transfer (first holder PAN) i.e., transfers made through account transfer cum closure module and with reason code transfer to own accounts. (Monthly frequency)</p>



Transaction Monitoring	TM 9C – Gift, Donation related off-market transfer	<ol style="list-style-type: none"> 1. Transaction value of such transaction is beyond 5 times of Income range / Net worth (as updated in demat account) on higher side as provided by the BO AND; 2. Listed Equity Shares will be considered AND; 3. Debit transaction specific reason codes > 5 lacs in value AND; 4. For Reason code /s -Family Account Transfer -Gift -Donation
	TM 9D – Off Market transfer at variance with market value	<ol style="list-style-type: none"> 1. Off market transfers with reason code “Off-Market Sale” And; 2. Difference of +/-50% difference in consideration value mentioned by BO and prevailing market value of Equity shares AND; 3. Only Listed Equity Share will be considered. AND; 5. Minimum transaction value for alert will be Rs 25lakhs;
	TM 9E – Off Market transfer in suspicious scrip	<ol style="list-style-type: none"> 1. Off market single or series of transactions having value of Rs 2 lakh and above AND; 2. Suspicious Scrips for which unsolicited SMSs were circulated will be taken from below URLs BSE:https://www.bseindia.com/attention_investores.aspx NSE:https://www.nseindia.com/regulations/unsolicitedmessages-report



Notes:

- ✓ Depository Participants have to generate alerts independently based upon the alert scenarios mentioned in TM9, TM9A, TM9B, TM9C, TM9D, TM9E and EI 9. Depository Participants have to undertake meaningful analysis, closure and filing of STRs of these alerts as defined under the PML rules.
- ✓ **Depositories were also advised to generate and forward alerts** to the depository participants **based upon the above alert scenarios** (TM9, TM9A, TM9B, TM9C, TM9D, TM9E and EI 9), which are mentioned as TM13, TM13A, TM13B, TM13C, TM13D, TM13E and EI13 in the '**Supplemental Guidelines for Detecting Suspicious Transaction for Depositories**' dated 21/07/2022.
- ✓ Alerts thus generated by the Depository Participants, need to be cross checked with the alerts being forwarded by the Depositories to ensure that all the alerts are carefully generated by the Depository Participants and meaningful analysis of these alerts have been conducted for detecting suspicious transactions.
- ✓ These RFI guidelines issued for the Depository Participants are common minimum alerts and parameters for generation of alerts. Depository Participants are advised to develop additional parameters for generation of additional alerts. Depository Participants can also set the thresholds depending upon the client profile. These thresholds are required to be reviewed periodically.
- ✓ The thresholds prescribed in these RFIs are indicative. Depository Participants are free to adopt stricter criteria thresholds, but may not adopt criteria less strict than that which is prescribed in these RFIs.

