

EQUIRUS SECURITIES PRIVATE LIMITED

ANTI MONEY LAUNDERING POLICY OF
EQUIRUS SECURITIES PVT. LTD.

INTRODUCTION TO AML

Being a SEBI registered intermediary it is mandatory to put in place a system for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities and a policy for ensuring that the anti-money laundering guidelines issued by SEBI from time to time are complied with.

The Directives as outlined below provide a general background and summary of the main provisions of the applicable anti-money laundering and anti-terrorist financing legislations in India. They also provide guidance on the practical implications of the Prevention of Money Laundering Act, 2002 (PMLA) and as amended from time to time. The Directives also set out the steps that shall be implemented to discourage and to identify any money laundering or terrorist financing activities. The relevance and usefulness of these Directives will be kept under review and it may be necessary to issue amendments from time to time.

These Directives are intended for use primarily by intermediaries registered under Section 12 of the Securities and Exchange Board of India Act, 1992 (SEBI Act). While it is recognized that a “one-size-fits-all” approach may not be appropriate for the securities industry in India, each registered intermediary shall consider the specific nature of its business, organizational structure, type of clients and transactions, etc. when implementing the suggested measures and procedures to ensure that they are effectively applied. The overriding principle is that they shall be able to satisfy themselves that the measures taken by them are adequate, appropriate and abide by the spirit of such measures and the requirements as enshrined in the PMLA.

Background of the Prevention of Money Laundering Act, 2002 (PMLA)

Global Framework:

In response to mounting concern over money laundering worldwide the G-7 Summit held in Paris in 1989 established a policy making body, having secretariat at Organisation for Economic Co-operation and Development (OECD), which works to generate the necessary political will to bring about national legislative and regulatory reforms to combat money laundering and terrorist financing.

The World Bank and the IMF have also established a collaborative framework with the FATF for conducting comprehensive AML/CFT assessments of countries' compliance with the FATF 40+8 Recommendations, using a single global methodology.

India has been accorded 'member' status.

Indian Framework:

The Prevention of Money Laundering Act, 2002 came into effect from 1st July 2005. Necessary notifications/ rules under the said Act were published in the Gazette of India on 1st July 2005 by the Dept of Revenue, Ministry of Finance, Government of India.

Subsequently, SEBI issued necessary guidelines vide circular no. ISD/CIR/RR/AML/1/06 dated 18th January 2006 to all securities market intermediaries registered under section 12 of the SEBI Act, 1992

Guidelines were issued in the context of recommendations made by the Financial Action Task Force (FATF) on anti-money laundering standards.

Applicability of PMLA Act

- Banking company
- Financial institution
- Intermediary (which includes a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with securities market and registered under Section 12 of the SEBI Act)
- All financial Intermediaries shall have to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules under the PMLA. Such transactions include:
 - All cash transactions of the value of more than 10 lakh or its equivalent in foreign currency.
 - All series of cash transactions integrally connected to each other which have been valued below 10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency.
- All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into from any non-monetary account such as demat account, security account maintained by the registered intermediary.

WHAT IS MONEY LAUNDERING?

Money Laundering involves disguising financial assets so that they can be used without detection of the illegal activity that produced them. Through money laundering, the launderer transforms the monetary proceeds derived from criminal activity into funds with an apparent legal source. Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities.

The term “Money Laundering” is also used in relation to the financing of terrorist activity (where the funds may, or may not, originate from crime). Money Laundering is a process of making dirty money look clean.

Money is moved around the financial system again and again in such manner that its origin gets hidden.

STAGES OF MONEY LAUNDERING

Although money laundering is a complex process, it generally follows three stages:

- Placement is the initial stage in which money from criminal activities is placed in financial institutions. One of the most common methods of placement is structuring—breaking up currency transactions into portions that fall below the reporting threshold for the specific purpose of avoiding reporting or recordkeeping requirements.
- Layering is the process of conducting a complex series of financial transactions, with the purpose of hiding the origin of money from criminal activity and hindering any attempt to trace the funds. This stage can consist of multiple securities trades, purchases of financial products such as life insurance or annuities, cash transfers, currency exchanges, or purchases of legitimate businesses.
- Integration is the final stage in the re-injection of the laundered proceeds back into the economy in such a way that they re-enter the financial system as normal business funds. Banks and financial intermediaries are vulnerable from the Money Laundering point of view since criminal proceeds can enter banks in the form of large cash deposits.

FINANCIAL INTELLIGENCE UNIT (FIU) INDIA

The Government of India has set up Financial Intelligence Unit (FIU-India) on November 18, 2004 as an independent body to report directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

FIU – India has been established as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspicious financial transactions. FIU India is also responsible for coordination and stretching efforts of national and international intelligence and enforcement agencies in pursuing the global efforts against money laundering and related crimes.

DEFINITIONS

“Beneficial Owner” means the natural person or persons who ultimately own, control or influence a Client and/or persons on whose behalf a transaction is being conducted including those persons who exercise ultimate effective control over a legal person or arrangement;

“Client” means an entity or person who is being provided services by ESPL.

PRINCIPAL OFFICER & DESIGNATED DIRECTOR - DESIGNATION AND DUTIES

ESPL has designated Mr. Vishad Turakhia as the Designated Director and Mr. Naman Shah as the Principal Officer for its anti-money laundering program (“AML” program), with full responsibility for the ESPL’s AML program. ESPL believes that both Designated Director and Principal Officer are qualified by experience, knowledge and training. The duties of the Principal Officer & Designated Director will include monitoring the ESPL’s compliance with AML obligations and overseeing communication and training for employees. The Principal Officer will also ensure that proper AML records are kept. When warranted, the Principal Officer will ensure filing of necessary reports with the Financial Intelligence Unit (FIU – IND).

ESPL has provided the FIU with contact information for the Principal Officer & Designated Director, including name, title, mailing address, e-mail address and telephone number. ESPL will promptly notify FIU of any change to this information.

POLICIES AND PROCEDURES TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

ESSENTIAL PRINCIPLES

SEBI Directives have taken into account the requirements of the PMLA as applicable to the intermediaries registered under Section 12 of the SEBI Act. The detailed Directives in Section II have outlined relevant measures and procedures to guide the registered intermediaries in preventing ML and TF. Some of these suggested measures and procedures may not be applicable in every circumstance. Each intermediary shall carefully consider the specific nature of its business, organizational structure, type of client and transaction, etc. to satisfy itself that the measures taken by it are adequate and appropriate and follow the spirit of the suggested measures in Section II and the requirements as laid down in the PMLA.

OBLIGATION TO ESTABLISH POLICIES AND PROCEDURES

Global measures taken to combat drug trafficking, terrorism and other organized and serious crimes have all emphasized the need for financial institutions, including securities market intermediaries, to

establish internal procedures that effectively serve to prevent and impede money laundering and terrorist financing. The PMLA is in line with these measures and mandates that all intermediaries ensure the fulfillment of the aforementioned obligations.

To be in compliance with these obligations, the senior management shall be fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. We shall:

- a. issue a statement of policies and procedures, on a group basis where applicable, for dealing with ML and TF reflecting the current statutory and regulatory requirements;
- b. ensure that the content of these Directives are understood by all staff members;
- c. regularly review the policies and procedures on the prevention of ML and TF to ensure their effectiveness. Further, in order to ensure the effectiveness of policies and procedures, the person doing such a review shall be different from the one who has framed such policies and procedures;
- d. adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF;
- e. undertake client due diligence (“CDD”) measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction;
- f. have in system a place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities; and
- g. develop staff members’ awareness and vigilance to guard against ML and TF.

Policies and procedures to combat ML shall cover:

- a. Communication of group policies relating to prevention of ML and TF to all management and relevant staff that handle account information, securities transactions, money and client records etc. whether in branches, departments or subsidiaries;
- b. Client acceptance policy and client due diligence measures, including requirements for proper identification;
- c. Maintenance of records;
- d. Compliance with relevant statutory and regulatory requirements;
- e. Co-operation with relevant law enforcement authorities, including timely disclosure of information; and
- f. Role of internal audit or compliance function to ensure compliance with the policies, procedures and controls relating to the prevention of ML and TF, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff, of their responsibilities in this regard. The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and other such factors.

The purpose of this document is to guide all the employees of Equirus Securities Pvt. Ltd. and employees of its associates on the steps that they are required to take and implement to prevent and identify any money laundering or terrorist financing activities. It shall be the responsibility of each of the concerned employees that they should be able to satisfy themselves that the measures taken by them are adequate, appropriate and follow the spirit of these measures and the requirements as enshrined in the “Prevention of Money Laundering Act, 2002”.

Some of these suggested measures may not be applicable to every circumstance or to each department, branch. However, each entity should consider carefully the specific nature of its business, type of customer and transaction to satisfy itself that the measures taken by the employees are adequate and appropriate to follow the spirit of these guidelines.

IMPLEMENTATION OF THIS POLICY

CLIENT DUE DELIGENCE

The CDD measures comprise the following:

The main aspect of this policy is the Customer Due Diligence Process which means:

- a. To obtain sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the Client, that party shall be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
- b. To verify the customer's identity using reliable, independent source document, data or information.
- c. To identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the Client and/or the person on whose behalf a transaction is being conducted;

For Clients other than individuals or trusts: Where the Client is a person other than an individual or trust, viz., company, partnership or unincorporated association/body of individuals, the intermediary shall identify the beneficial owners of the Client and take reasonable measures to verify the identity of such persons, through the following information:

- a. The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

Explanation: Controlling ownership interest means ownership of/entitlement to:

- i. more than 10% of shares or capital or profits of the juridical person, where the juridical person is a company;
 - ii. more than 10% of the capital or profits of the juridical person, where the juridical person is a partnership; or
 - iii. more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.
- b. In cases where there exists doubt under clause above as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.

Explanation: Control through other means would include exercised through voting rights, agreement, arrangements or in any other manner.

- c. Where no natural person is identified under any of clauses above, the identity of the relevant natural person who holds the position of senior managing official.

For Client which is a trust: Where the Client is a trust, the Company shall identify the beneficial owners of the Client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

Exemption in case of listed companies: Where the Client or the owner of the controlling interest is a Company listed on a Stock Exchange, or is a majority-owned subsidiary of such a Company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

If the client is Non-Profit organization: The details of a client, to be registered on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and the registered intermediary has ended or the account has been closed, whichever is later.

Applicability for foreign investors: Dealing with foreign investors' may be guided by the clarifications issued vide SEBI Master circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19, 2022 and amendments thereto, if any, for the purpose of identification of beneficial ownership of the Client.

- d. To verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c); and
- e. To understand the ownership and control structure of the Client.
- f. To conduct ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the Client, its business and risk profile, taking into account, where necessary, the Client's source of funds; and
- g. To periodically update all documents, data or information of all Clients and beneficial owners collected under the CDD process.

Where registered intermediary is suspicious that transactions relate to money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the client, the registered intermediary shall not pursue the CDD process, and shall instead file a STR with FIU-IND

Reliance on third party for carrying out Client Due Diligence (CDD)

Trading Member may rely on a third party for the purpose of (a) identification and verification of the identity of a client and (b) determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act. Further, it is

clarified that the Company shall be ultimately responsible for Client Due Diligence (CDD) and undertake enhanced due diligence measures, as applicable.

CLIENT ACCEPTANCE POLICY

Client acceptance policies and procedures aim to identify the types of Clients that are likely to pose a higher than average risk of ML or TF. To apply Client due diligence on a risk sensitive basis depends on the type of Client business relationship or transaction. The following safeguards shall be followed by the Company while accepting the Clients:

- No account is opened in a fictitious/benami name or on an anonymous basis;
- Factors of risk perception (in terms of monitoring suspicious transactions) of the Client shall be defined having regard to Clients' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. The parameters shall enable classification of Clients into low, medium and high risk. Clients of special category (as given below) may, if necessary, be classified even higher. Such Clients require higher degree of due diligence and regular update of Know Your Client (KYC) profile.
- Documentation requirements and other information to be collected in respect of different classes of Clients shall depend on the perceived risk and having regard to the requirements of Rule 9 of the PML Rules, directives and circulars issued by SEBI from time to time.
- To ensure that an account is not opened where the Company is unable to apply appropriate CDD measures/KYC policies. It shall apply in cases where it is not possible to ascertain the identity of the Client, or the information provided to the intermediary is suspected to be non - genuine, or there is perceived non co-operation of the Client in providing full and complete information. In such a case, the Company shall continue to do business with such a person and file a suspicious activity report. The Company shall also evaluate whether there is suspicious trading in determining whether to freeze or close the account. A cautious step shall be taken to ensure that we do not return securities of money that may be from suspicious trades. The Company shall consult the relevant authorities in determining what action shall be taken when suspicious trading is suspected.
- Do not accept Clients with identity matching with a person known to have criminal background: To check whether the Client's identity matches with any person known to be having criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement/regulatory agency worldwide.

RISK – BASED APPROACH

It is generally recognized that certain Clients may be of a higher/lower risk category depending on the circumstances such as Client's background, type of business relationship or transaction etc. As such, each of the Clients due diligence measures on a risk sensitive basis shall be applied. The basic principle preserved in this approach is that an enhanced CDD process shall be adopted for higher risk categories of Clients. Conversely, a simplified Client due diligence process may be adopted for lower risk categories of Clients. In line with the risk-based approach, the type and amount of identification information and documents that shall be obtained necessarily would depend on the risk category of a particular Client.

Further, low risk provisions shall not be applied when there are suspicions of ML/FT or when other factors give rise to belief that customer does not in fact pose a low risk.

RISK ASSESSMENT

Risk assessment to be carried out to identify, assess and take effective measures to mitigate money laundering and terrorist financing risk with respect to clients, countries or geographical areas, nature and volume of transactions, payment methods used by Clients, etc. The risk assessment shall also take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions. These shall be accessed by the company at the URL

- http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml
- <http://www.un.org/sc/committees/1988/list.shtml>

The risk assessment carried out shall also consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. The assessment shall be documented, updated regularly and made available to competent authorities and self regulating bodies, as and when required by them.

To identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products and also ensure:

- a. To undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
- b. Adoption of a risk based approach to manage and mitigate the risks”.

RISK CLASSIFICATION

The level of Money Laundering (ML) risks that ESPL is exposed to by an investor relationship depends on:

1. Type of the customer and nature of business
2. Type of product/service availed by the customer
3. Country where the Customer is domiciled

Based on above criteria, clients may be classified in three money laundering categories:

i. Low Risk (Level I):

Following Individuals and entities can be categorized as low risk clients:

- Whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile.
- Individuals/Corporate/HNIs who have respectable social and financial standing.
- Where the client profile according to the perception of the ESPL is certain.
- The illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Further low risk provisions should not apply

when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not in fact pose a low risk.

ii. Medium Risk (Level II):

Customers that are likely to pose a higher than average risk to ESPL may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc; such as:

Persons in business/industry or trading activity where the area of his residence or place of business has a scope or history of unlawful trading/business activity.

Where the client profile of the person/s opening the account, according to the perception of the Member is uncertain and/or doubtful/dubious.

iii. High Risk (Level III):

ESPL may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear or are from high risk countries or geographic area. In such cases, ESPL shall verify the clients identity taking into consideration the type of client, business relationship, source of fund, nature and value of transactions based on overall money laundering and terrorist financing risks involved. The examples of customers requiring enhanced due diligence may include:

- Non Resident Customers,
- High Net worth individuals whose profile is uncertain according to Members' perception.
- Trusts, charities, NGOs and organizations receiving donations,
- Firms with 'sleeping partners'
- Politically Exposed Persons (PEPs) of foreign origin
- Family members or close relatives / associates of PEPs.
- Natural and legal persons (including financial institutions) from countries for which EDD is called for by FATF.
- Non-face to face customers, and

Those with dubious reputation as per public information available, etc.

CLIENTS OF SPECIAL CATEGORY

Utmost care shall be taken while dealing with a Client of Special Category. Such Clients shall include:

NRIs, HNIs, Trust, Charities, NGOs, Organization receiving Donation, Politically Exposed Persons (PEP) including their family and close relatives, Persons of Foreign Origin, Companies having closed Shareholding/Ownership, Companies dealing in Foreign Currency, Shell Companies, Overseas Entities, Clients in high risk countries, Non face to face Clients and Clients with dubious background. Current/Former Head of State, Current/Former senior high profile politician, Companies offering Foreign Exchange, etc. or Clients from high-risk countries where existence/effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, countries active in narcotics production, countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, countries against which government sanctions are applied, countries reputed to be any of the following – Havens/sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent. While dealing with Clients in high risk countries other than FATF

recommendations, published by the FATF on its website (www.fatf-gafi.org), we shall also independently access and consider other publicly available information.

CLIENT IDENTIFICATION PROCEDURE

The procedure shall include

- a. To put in place appropriate risk management systems to determine whether the Client or potential client or the beneficial owner of such Client is a politically exposed person. Such procedures shall include seeking relevant information from the Client, referring to publicly available information or accessing the commercial electronic databases of PEPS. Further, the enhanced CDD measures as outlined in clause above shall also be applicable where the beneficial owner of a Client is PEP. Also Applying the same norms applicable to Politically Exposed Persons (PEPs) to *their family members or close relatives*.
- b. Senior management approval shall be obtained for establishing business relationships with PEPs. Where a Client has been accepted and the Client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, senior management approval to be obtained to continue the business relationship.
- c. Reasonable measures to be taken to verify the sources of funds as well as the wealth of Clients and beneficial owners identified as PEP.
- d. The Client shall be identified by using reliable sources including documents/information. Adequate information shall be obtained to satisfactorily establish the identity of each new Client and the purpose of the intended nature of the relationship.
- e. Adequate information shall be kept so as to satisfy competent authorities (regulatory/enforcement authorities) in future that due diligence was observed by the Company in compliance with these directives. Each original document shall be seen prior to acceptance of a copy.
- f. Failure by prospective Client to provide satisfactory evidence of identity shall be noted and reported to the higher authority/senior management.

An ongoing due diligence shall be conducted where inconsistencies in the information provided by the Client has been identified. The underlying objective shall be to follow the requirements preserved in the PMLA, SEBI Act and regulations, directives and circulars issued, so as to be aware of the Clients on whose behalf the Company is dealing.

It may be noted that irrespective of the amount of investment made by Clients, no minimum threshold or exemption is available from obtaining the minimum information/documents from Clients as stipulated in the PML Rules/SEBI Circulars (as amended from time to time) regarding the verification of the records of the identity of Clients. Further no exemption from carrying out CDD exists in respect of any category of Clients. In other words, there shall be no minimum investment threshold/category-wise exemption available for carrying out CDD measures.

RECORD KEEPING REQUIREMENTS & RETENTION OF RECORDS

Records pertaining to transactions of Clients shall be maintained and preserved for a period of eight years for DP and five years for Stock Market from the date of the transaction. Record of documents evidencing the identity of the Clients and beneficial owners (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents) as well as account files and business correspondence shall be maintained and preserved for a period of eight years for DP and five years for Stock Market even after the business relationship with the Client has ended or the account has been closed, whichever is later. Records shall be maintained as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior or if there be any suspected drug related or other laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, the following information of the Client shall be maintained in order to maintain a satisfactory audit trail:

- a. the beneficial owner of the account;
- b. the volume of the funds flowing through the account; and
- c. for selected transactions:
 - i. origin of the funds;
 - ii. form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.;
 - iii. identity of the person undertaking the transaction;
 - iv. destination of the funds; and
 - v. form of instruction and authority.

System is been maintained to record all such transaction as prescribed under Rule 3 of the PML Rules as follows:

- a. all cash transactions of the value of more than Rs. 10 lacs or its equivalent in foreign currency;
- b. all series of cash transactions integrally connected to each other which have been individually valued below Rs. 10 lacs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of Rs. 10 lacs or its equivalent in foreign currency;
- c. all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;
- d. all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

Record of information related to transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 & 8 of the PML Rules, shall be maintained and preserved for a period of eight years for DP and five years for Stock Market from the date of the transaction with the Client.

In the case of transactions where any investigations by any authority has been commenced and in the case of transactions which have been the subject of suspicious transactions reporting all the records shall be maintained till the authority in forms of closure of the case.

INFORMATION TO BE MAINTAINED

Following information in respect of transactions referred to in Rule 3 of PML Rules shall be maintained:

- a. the nature of the transactions;
- b. the amount of the transaction and the currency in which it is denominated;
- c. the date on which the transaction was conducted; and
- d. the parties to the transaction.

MONITORING OF TRANSACTIONS

Special attention shall be paid to all complex unusually large transactions/patterns which appear to have no economic purpose. Internal threshold limits for each class of Client accounts shall be defined and special attention shall be paid to transactions which exceeds these limits.

The background including all documents/office records/memorandums/clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records and related documents shall be made available to auditors and also to SEBI/Stock Exchanges/FIU-IND/other relevant authorities, during audit, inspection or as and when required. These records shall be preserved for a period of eight years for DP and five years for Stock Market from the date of transaction with such Client.

Record of the transactions in terms of Section 12 of the PMLA shall be preserved and those transactions of a suspicious nature or any other transactions notified under Section 12 of the Act shall be reported to the Director, FIU-IND. Suspicious transactions shall be regularly reported to the Senior Management.

SUSPICIOUS TRANSACTION MONITORING AND REPORTING

All are requested to analyze and furnish details of suspicious transactions, whether or not made in cash. It should be ensured that there is no undue delay in analysis and arriving at a conclusion.

What is a Suspicious Transaction?

- Clients whose identity verification seems difficult or Clients appear not to co-operate;
- Substantial increase in activity without any apparent cause;
- Large number of accounts having common parameters such as common partners/directors/promoters/address/email address/telephone numbers/introducers or authorized signatories;
- Transactions with no apparent economic or business rationale;
- Sudden activity in dormant accounts;
- Source of funds are doubtful or inconsistency in payment pattern;
- Unusual and large cash deposits made by an individual or business;
- Transfer of investment proceeds to apparently unrelated third parties;
- Multiple transactions of value just below the threshold limit of Rs. 10 lacs specified in PMLA so as to avoid possible reporting;

- Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- Purchases made on own account transferred to a third party through off market transactions through DP accounts;
- Suspicious off market transactions;
- Large deals at prices away from the market;
- Accounts used as 'pass through'. Where no transfer of ownership of securities or trading is occurring in the account and the account is being used only for funds transfers/layering purposes;
- All transactions involving receipts by non-profit organizations of value more than Rs. 10 lacs or its equivalent in foreign currency;
- Clients of high risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards, as 'Clients of Special Category'. Such Clients should also be subject to appropriate counter measures. These measures may include a further enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or systematic reporting of financial transactions, and applying enhanced due diligence while expanding business relationships with the identified country or persons in that country etc.

Irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in Part B of Schedule of PMLA, 2002, file STR if we have reasonable grounds to believe that the transactions involve proceeds of crime."

What to Report?

- Any suspicious transaction shall be immediately notified to the Money Laundering Control Officer, Compliance Officer, Principal Officer or any other Designated Officer.
- The notification may be done in the form of a detailed report with specific reference to the Clients, transactions and the nature/reason of suspicion.
- In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken.
- The Principal Officer/Money Laundering Control Officer and other appropriate compliance, risk management and related staff members shall have timely access to Client identification data and CDD information, transaction records & other relevant information.
- It is likely that in some cases transactions are abandoned or aborted by Clients on being asked to give some details or to provide documents.
- It is clarified that intermediaries should report all such attempted transactions in STRs, even if not completed by Clients, irrespective of the amount of the transaction.

LIST OF DESIGNATED INDIVIDUALS OR ENTITIES

An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at <http://www.un.org/sc/committees/1267/consolist.shtml>

Precaution shall be taken to ensure that no account is opened whose name shall be appearing in such list. Periodic review of the existing account shall be conducted to ensure that no existing accounts are linked to any of the entity or individual included in the list.

Any resemblance found shall be reported to SEBI and FIU-IND.

PROCEDURE FOR FREEZING OF FUNDS, FINANCIAL ASSETS OR ECONOMIC RESOURCES OR RELATED SERVICES

14.1 Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA), relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government has issued an order dated August 27, 2009 detailing the procedure for the implementation of Section 51A of the UAPA.

14.2 Under the aforementioned section, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed in the Schedule to the order, or any other person engaged in or suspected to be engaged in terrorism. The Government is also further empowered to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the order or any other person engaged in or suspected to be engaged in terrorism.

14.3 On receipt of the updated list of individuals/entities subject to UN sanction measures (hereinafter referred to as 'list of designated individuals/entities) from SEBI/Stock Exchange:

- a. to verify whether individuals or entities listed in the Schedule to the order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of securities with us.
- b. In the event, particulars of any of customer/s match the particulars of designated individuals/entities, we shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of securities, held by such customer in our books to the Joint Secretary, Ministry of Home Affairs at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post shall compulsorily be conveyed through e-mail at jsis@nic.in
- c. We shall send the particulars of the communication mentioned in (b) above through post/fax and through e-mail (sebi_uapa@sebi.gov.in) to the UAPA Nodal Officer of SEBI, Officer on Special Duty, Integrated Surveillance Department, Securities and Exchange Board of India, SEBI Bhavan, Plot No. C4-A, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051 as well as the UAPA Nodal Officer of the State/UT where the account is held, as the case may be, and to FIU-IND.
- d. In case the aforementioned details of any of the customers match with the particulars of designated individuals/entities beyond doubt, we shall prevent such designated persons from conducting financial transactions, and at the same time intimation will be sent to Joint Secretary, Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-

23092736. The particulars apart from being sent by post shall compulsorily be conveyed through e-mail at jsis@nic.in

- e. We shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts.

14.4 Implementation of requests received from foreign countries under U.N. Securities Council Resolution 1373 of 2001

- i. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities.
- ii. To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA Nodal Officer for IS-I division for freezing of funds or other assets.
- iii. The UAPA Nodal Officer of IS-I Division of MHA, shall cause the request to be examined, within five working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the Nodal Officer in SEBI. The proposed designee, as mentioned above would be treated as designated individuals/entities.
- iv. Upon receipt of the requests from the UAPA Nodal Officer of IS-I Division, the procedure as enumerated at paragraphs 15.3 above shall be followed.

14.5 Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person:

Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, shall move an application giving the requisite evidence, in writing, to the concerned stock exchanges/depositories and to us. On receipt of such request, we shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the Nodal Officer of IS-I Division of MHA as per the contact details given within two working days. The Joint Secretary (IS-I), MHA, being the Nodal Officer for (IS-I) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned stock exchanges, depositories and registered intermediaries. However, if it is not possible for any reason to pass an order

unfreezing the assets within fifteen working days, the Nodal Officer of IS-I Division shall inform the applicant.

REPORTING TO FIU

In terms of the PMLA rules, brokers and sub-brokers are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND), 06th Floor, Hotel Samarat, Chanakyapuri, New Delhi – 110 021 as per the schedule given below:

Report	Description	Due Date
CTR	All cash transactions of the value of more than Rs. 10 lacs or its equivalent in foreign currency; and All series of cash transactions integrally connected to each other which have been valued below Rs. 10 lacs or its equivalent in foreign currency where such series of transactions have taken place within a month	15th day of the succeeding month
STR	All suspicious transactions whether or not being made in cash	Not later than seven days on satisfied that the transaction is suspicious
NTR	Non-Profit Organization Transaction Report	15th day of the succeeding month

Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND. Utmost confidentiality shall be maintained in filing of CTR, STR and NTR to FIU-IND. No NIL reporting needs to be made to FIU-IND in case there are no cash/suspicious/non-profit organization transactions to be reported.

Irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in the PMLA, 2002, an STR shall be filed, if there is reasonable grounds to believe that the transactions involves proceeds of crime.

PRINCIPAL OFFICER

The Company has designated the Principal Officer who shall be responsible for implementation and compliance of this policy shall include the following:

- Compliance of the provisions of the PMLA and AML guidelines;
- Monitoring the implementation of Anti Money Laundering (AML) and Combating Financing of Terrorism (CFT) Policy;
- Reporting of transactions and sharing of information as required under the law;
- Ensuring submission of periodical reports to top management. The report shall mention if any suspicious transactions are being looked into by the respective business groups and if any reporting is to be made to the authorities; and
- Ensure that Equirus Securities Pvt. Ltd. discharges its legal obligation to report suspicious transactions to the concerned authorities.

DESIGNATED DIRECTOR

“Designated Director” means a person designated by the Board of Directors to ensure overall compliance with the obligations imposed under Prevention of Money Laundering Act, 2002 and the Rules framed there under, as amended from time to time, and include Managing Director or Whole-time Director duly authorized by Board of Directors. The Company shall appoint a Designated Director and communicate the details of the Designated Director, such as name, designation & address to the Office of Director, FIU-IND & update same whenever there is any change.

DETAILS OF DESIGNATED DIRECTOR & PRINCIPAL OFFICER

Name	Vishad Turakhia	Naman Shah
Designation	Designated Director	Principal Officer
Office address	21 st Floor, A Wing, Marathon Futurex, N. M. Joshi Marg, Lower Parel, Mumbai – 400 013.	House No. 9, 03 rd Floor, Magnet Corporate Park, Near Zydus Hospital, S. G. Highway, Ahmedabad – 380 054.
Telephone No.:	022 4332 0600	079 6190 9561
Mobile No.	+91 98334 64564	+91 7069030851
Email ID	vishad.turakhia@equirus.com	naman.shah@equirus.com

SYSTEM AND PROCEDURE FOR HIRING OF EMPLOYEES

- i. Department Heads shall be involved in hiring of new employees, shall adequately carry out the screening procedure in place to ensure high standards in hiring new employees.
- ii. Bona fides of employees are checked to ensure that the employees do not have any link with terrorist or other anti-social organizations.
- iii. Reference of candidate: Candidate having reference would be called for the interview. In case of employee having applied through newspaper would be called for the interview after scrutinizing his/her bio-data.
- iv. Background of Candidate: Background of the employee should be clean & under no circumstances candidate who has left earlier employer due to dispute should be selected.
- v. Third party verification of Candidate: If necessary third party verification should be done by making phone call.
- vi. Experience: Candidate should have to appear for the skilled test depending on the exposure.
- vii. Candidate should be aware for PMLA 2002 guidelines. Proper training should be given if he/she is not aware.

EMPLOYEES TRAINING

- Importance of PMLA Act and its requirement to employees through training.
- Ensuring that all the operating and management staff fully understands their responsibilities under PMLA for strict adherence to customer due diligence requirements from establishment of new accounts to transaction monitoring and reporting suspicious transactions to the FIU.
- Organizing suitable training programmes wherever required for new staff, front line staff, supervisory staff, etc.
- Briefings to new employees at induction programs and rounds of small meetings and presentations at branch locations.

- Adequate training should be given to all the concerned employees to (a) ensure that the contents of the guidelines are understood and (b) develop awareness and vigilance to guard against money laundering and terrorist financing.
- As of now, AML policy will be covered during the induction training given to all new recruits and also during the on-going compliance sessions.

INVESTORS EDUCATION

As the implementation of AML/CFT measures being sensitive subject and requires us to demand and collect certain information from investors which may be of personal in nature or has hitherto never been called for, which information include documents evidencing source of funds/income tax returns/bank records etc. and can sometimes lead to raising of questions by the Client with regard to the motive and purpose of collecting such information. There is, therefore, a need for us to sensitize the Clients about these requirements, as the ones emanating from AML and CFT framework. We shall circulate the PMLA Circulars and other specific literature/pamphlets etc. so as to educate the Client of the objectives of the AML/CFT program. The same shall also be emphasized on, in the Investor Awareness Programs conducted by us at frequent intervals of time. The importance of the same is also made known to them at the time of opening the account.

REVIEW OF THE POLICY

This Policy shall be reviewed annually or as required to incorporate and implement the amendments in the PMLA or relevant circulars.



EQUIRUS SECURITIES PRIVATE LIMITED

RISK MANAGEMENT & INTERNAL CONTROL

POLICY

Risk Management Policy

The Risk management policy is developed by us considering the rules and circulars as issued by the SEBI/Exchanges time to time. The said policy is subject to change as per rules/regulation issued by SEBI/Exchange and also as per the ruling market environment. Salient features of the policy are as follow.

DEFINITIONS

- RMS: Risk Management System-helps to manage the risk of the company and client from volatility and market risks.
- Cash: The clear balance available in client's ledger account in the books of the company.
- Margin: The underlying stake provided by the client in the form of cash, FDR and / or pledged stock to mitigate market (price) or settlement (auction) risk.
- Exposure: The aggregate of the customer's obligations arising out of buy and sell trades awaiting settlement in the cash segment and profit/ loss amounts that are yet to be settled on the closed positions including future and options.

EXPOSURES

Exposure are allotted to the clients on the basis of his available ledger balance and/or margin pledge securities with us. For this purpose, available securities are valued using previous days closing price. Haircut is then applied, VaR margin rate, to this value. Sum of available ledger balance and residual securities value, after applying haircut, is the Exposure limit of the client for Cash segment. In case of F&O segment, besides the aforesaid items. We accept only those



securities which are accepted by the exchange against margin obligation of F&O segment. These securities are also valued after applying proper haircut as instructed by the exchange.

MARGIN:

Aforesaid exposure allotted to client, is subject to VAR, Extreme loss margin and other margins as charged by the exchange. RMS team on its own discretion can impose additional Margin or increase the margin and can also increase the haircut on script on its risk preparations subject to market conditions and other relevant factors like market volatility etc.

DISCRETIONS ON LIMITS:

- (i) Equirus Securities Private Limited has discretion to change the limits on the basis of risk perception and other factors Considered relevant (such as broker level/exchange level limits in specific securities or Income declaration or volume Specific exposures based on surveillance measures)
- (ii) Equirus Securities Private Limited shall not be able to inform the client of such variation, reduction or imposition in advance.
- (iii) Equirus Securities Private Limited shall not be responsible for client's inability to execute any order on account of any such variation, reduction or imposition of limits.

CONTROLLING

Controlling function is done by the Risk management department. The concerned executive is authorized for allowing exposure limit to the client. The concerned group executive considers the group net position, available exposure limit of the client and as well as the past record of the concerned group and client for deciding the exposure limit. It is at the sole discretion of the group executive to allow/disallow the request of client for extra exposure limit. In case the group



executive faces some problem he/she forwards the matter to his/her senior for taking the appropriate decision.

PAY-IN / PAY-OUT OF FUNDS AND SECURITIES

Pay-in amount of clients is collected at regular basis. If there is debit ledger balance the securities purchased by the clients-pledge will be marked for such securities. If client fulfills his pay-in obligation the securities are shall be released form pledge.

MONITORING

Risk management department monitors obligation and positions of the clients. In case the client fails to clear his debit or obligation, liquidation or square off will be initiated.

Delay Payment Penalty shall be chargeable @18% p.a. on outstanding debit from the date of debit.

In the market event, Equirus Securities Private Limited has the risk perception that further trading in the securities /contracts may not be allowed to its clients and/or the market for trade or further position.

THE RIGHT TO SELL CLIENTS SECURITIES OR CLOSE CLIENT'S POSITIONS, WITHOUT GIVING NOTICE TO THE CLIENT, ON ACCOUNT OF NON-PAYMENT OF CLIENTS DUES

Equirus Securities Private Limited shall have the right to sell client's securities, both unpaid securities as well as collaterals deposited towards margins, or close out client's open positions,



without giving notice to the client where there is a delay /failure of the client to the pay-in obligations and/or there is a failure of the client to bring Margins and/ or additional margins to cover the increase in risk in the market conditions.

Equirus Securities Private Limited shall not be responsible for any losses and penalties / charges levied by exchanges(s) caused on such square off.

Equirus Securities Private Limited therefore not be under any obligation to compensate / or provide reasons for any delay or omission on its part to sell clients securities or close open positions of the client.

ILLIQUID CONTRACTS.

RMS shall have absolute discretion to accept, refuse or partially accept any order for execution from a client in respect of penny stocks, illiquid stocks, stocks having low liquidity, illiquid “options”, far month “options”, writing of “options”, and any other contracts which as per the perception of ESPL are extremely volatile or subject to Market manipulation. Exchange launches contracts from time to time for trading in derivatives and further the liquidity of these contracts is monitored time to time on the basis of their trading volume and availability of buyers and sellers. Trades of the clients on these contracts are blocked /unblocked at our trading /RMS team/software accordingly. The Concerned officer will be made responsible to monitor every new launched contract and will be responsible to block the same from its back end immediately. When liquidity comes to these contracts the responsibility of the executive will be to unblock the same for trading purposes and/or if any client willingly to trade in these illiquid contracts, he will immediately refer the matter to its RMS Head. RMS head will permit client after monitoring his trades and volumes and will permit the client to further trade in these contracts with caution.

The client itself will be liable for the loss incurred in such trades and Equirus Securities Private Limited shall not be responsible for delay in execution of such orders and consequential



opportunity loss or financial loss to the client. Equirus Securities Private Limited shall have the prerogative to place such restrictions, notwithstanding the fact that the client has adequate credit balance or margin available in his account and/or the client had previously purchased or sold such securities/contracts through Equirus Securities Private Limited itself.

PENALTY LEVIED BY CLEARING CORPORATIONS ON SHORT/NON-COLLECTION OF UPFRONT MARGINS

As per the Exchange Circular, penalty levied by clearing corporations on short/non-collection of upfront margins may be passed on to the client, if short/non collection of upfront margins is on account of following reasons attributable to client:

- I. Cheque issued by client to trading member is dishonoured
- II. Increase in margins on account of change in hedge position by client/ expiry of some leg(s) of the hedge positions of the clients.

The said policy is a part of company's Risk Management Policy and shall be reviewed along with the said policy on a yearly basis.

SURVEILLANCE POLICY

1. Objective

In accordance with BSE Notice No. 20130307-21 dated March 07, 2013 and NSE Circular Ref. no. NSE/INVG/22908 dated March 07, 2013 trading members are required to frame surveillance policy for handling effective monitoring of trading activity of client. In compliance with the aforesaid circulars, Equirus Securities Private Limited (hereinafter referred to as ESPL) adopts and implements below mentioned Surveillance Policy covering areas mentioned in the aforementioned circular which is approved by its Board of Directors in their meeting held on September 20, 2024 at the Registered Office of ESPL:

2. What is Surveillance?

Surveillance is the process of collecting and analyzing information concerning markets in order to detect unfair transactions that may violate securities related laws, rules and regulations. In order to ensure investor protection and safeguard the integrity of the markets, it is imperative to have in place an effective market surveillance mechanism. The main objective of surveillance function is to help maintain a fair and efficient market for securities.

3. Receipt of Alerts from Exchanges / generated on E-Boss & ENIT

In order to facilitate effective surveillance mechanisms at the Member level, the the Stock Exchanges viz. NSE and BSE are providing alerts based on predefined criteria to the all the stock brokers including EQUIRUS SECURITIES PRIVATE LIMITED through their portals.

Exchanges provides mandatory transactional alerts along with other alerts to the trading members through e-BOSS (BSE) and ENIT (NSE). The same has been listed out here below.

As per applicable Circulars, EQUIRUS SECURITIES PRIVATE LIMITED is reviewing these alerts and taking appropriate actions after carrying out due diligence viz. either disposing off alerts with appropriate reasons/findings recorded or filing Suspicious Transaction Report (STR) with FIU-India in accordance with provisions of PMLA (Maintenance of records) Rules,2005.

Sr. No.	Transactional Alerts	Segment
1	Significantly increase in client activity	Cash
2	Sudden trading activity in dormant account	Cash

3	Clients/Group of Client(s), dealing in common scrips	Cash
4	Client(s)/Group of Client(s) concentrated in a few illiquid scrips	Cash
5	Client(s)/Group of Client(s) dealing in scrip in minimum lot size	Cash
6	Client / Group of Client(s) Concentration in a scrip	Cash
7	Circular Trading	Cash
8	Pump and Dump	Cash
9	Wash Sales	Cash & Derivatives
10	Reversal of Trades	Cash & Derivatives
11	Front Running	Cash
12	Concentrated position in the Open Interest / High Turnover concentration	Derivatives
13	Order book spoofing i.e. large orders away from market	Cash

BSE – Alerts can be downloaded by log-in into e-Boss Surveillance System.

NSE - Alerts can be downloaded by log-in into ENIT- ENIT Compliance- Investigation Department – Transactional Alerts.

4. **Suspicious / Manipulative activity identification and reporting process**

Suspicious / Manipulative activity identification and reporting process include gathering of client information, analysing client activity, seeking documentary evidence required, monitoring the trading activities, record maintenance and reporting.

4.1 Client Information

- Implementing Anti Money Laundering Policy viz a viz KYC standard for new clients acceptance and implementing high standard of due diligence process.
- Periodic updating of client database and having system to do continues due diligence.
- Identification of Beneficial Ownership
- Identification of Multiple Accounts/common Accounts/group of clients
- Analysing common emails, mobile numbers, address and other linkages
- Other publicly available information

4.2 Analysing Client Activity

Client' trading pattern or activity shall be analysed based on Alert received/generated through exchange system. There are alerts which require only client confirmation or explanation or trading history analysis and there are other alerts which require documentary evidence viz. Bank Statement or Demat Statement for +/- 15 days as per Exchange requirements.

- Transaction Alerts falling under Sr. No. 1 & 2

It requires only trading history analysis, last 12 months trading turnover analysis, turnover v/s income range comparison and client confirmation on sudden activity in dormant account. Member shall also take reasonable steps to analyse these type of alerts and shall be required to close the status of alerts or report the exchange in case of any adverse findings.

- In case of transactional alerts from Sr. No. 3 to 13,

Apart from analysing trading history and income comparison, member shall take explanations regarding alerts received from the exchange and also ask for +/- 15 Days Bank Statement in case of Funds Movement and Demat Statement in case of movement of shares and Compliance Manager/Operation Manager shall verify whether the funds/securities for the settlement of such trades actually belongs to the client for whom the trades were transacted or not.

Members shall record observation for such transactional alerts and maintain records with regards to such analysis. In case, client failed to provide explanation or documentary evidences, such client shall be deactivated and shall be activated only after they satisfy all requirement of this policy.

5. Time frame for disposition of alerts

All the alerts downloaded will be analysed by Operations Manager & Compliance Manager keeping in view category of Client Type, Risk Categorisation, Income Range selected and Past Trading Pattern of each category. In case of any adverse findings, same shall be informed to Exchange with comments within 45 days of receipt of Alert. If there is any delay in disposition, written extension to be taken from respective exchange and reason for the same shall be documented.

6. Record Maintenance

Member shall record observation for such transactional alerts and maintain record with regard to such analysis. Record must be maintained as per statutory time frame. A quarterly MIS shall be put up to the Board in case of any adverse findings for further action.

7. Supervision of Compliance Officer

In case of any alert downloaded which is suspicious, same shall be informed to Compliance Officer. Any Corrective measures/action to be taken shall be under the supervision of Compliance Officer. Compliance officer shall be responsible for all surveillance activities carried out and for the record maintenance and reporting of such activities.

8. In addition to the above alerts, EQUIRUS SECURITIES PRIVATE LIMITED has framed its Surveillance Policy for Stock Broking to generate alerts as per guidance provided by SEBI/Exchanges. The same has been listed out below:

- 8.2.1.1.** Trading activity in a single day by one client or group of clients who have contributed more than 5% in a single scrip or a single derivative contract.
- 8.2.1.2.** A client or a group of clients who are either new client/ clients or who have reactivated their trading account after significant time gap and who have contributed more than 10% of the total trading volume of a single scrip or derivative contract in a single day.
- 8.2.1.3.** Client or a group of clients dealing frequently in small quantities. Minimum market lot in a scrip/contracts.
- 8.2.1.4.** Trading activity of a client found to be disproportionate considering a reported income range detail or net worth.
- 8.2.1.5.** A client who has submitted frequent modification request for changes in his/her/its demographic details of address, email id, mobile number, bank details etc.
- 8.2.1.6.** A client or a group of clients who have been found to have direct or indirect connection with a listed company and who have executed any transactions prior to any dissemination of any price sensitive information by such listed company.
- 8.2.1.7.** A client or group of clients having more than 10% volume of any scrip listed in for 'information list' or 'current watch list'.
- 8.2.1.8.** A client or group of clients which persistently earn or incur high amount of Profit/loss through their trading activities or clients who appear to have executed trades with the objective of transfer of profits or losses.
- 8.2.1.9.** A client who is having turnover more than 10% of the total turnover of the script and has pledged of his/her/it's such holding for

margin purpose and who has also significant trading volume in the same scrip which he/she/it holds.

- 8.2.1.10.** In case of a client or a group of clients who have been identified as per any of the above 9 criteria and whose orders are placed through a dealing office which is far from such client's address as per his/her/its KYC.
- 8.2.1.11.** A client having demat account with EQUIRUS SECURITIES PRIVATE LIMITED and who has holding in a scrip of more than 5% of paid up capital of a listed company which has received the same shares through off-market transfer.
- 8.2.1.12.** A client who has received shares of a listed company through multiple off-market transfer and has pledged such shares.
- 8.2.1.13.** Identification of IP addresses of clients to identify multiple client codes trading from same IP address.
- 8.2.1.14.** Clients who are connected with each other as per key KYC parameters of the clients as updated by respective client.

- a.** The stock broking operation shall review the alerts provided by Stock Exchanges on an ongoing basis and shall ensure to process the same as early as possible. In any case, these alerts will be processed within 45 days from the date of generation of the alert by the Stock Exchanges.

In case of any delay in disposing off any alerts, reasons for the same shall be recorded.

- b.** The stock broking operation shall, in case of reporting of any transaction as STR to FIU-India, shall evaluate whether any further action including suspension of the trading activity of the suspect client(s), reporting to Stock Exchanges/SEBI and/or other Regulatory Authorities.
- c.** The stock broking operation shall maintain records for such period as is prescribed under PMLA (Maintenance of Records) Rules, 2005, and Securities Contracts (Regulation) Rules, 1957 and any other directions as may be issued by SEBI/ Stock Exchanges from time to time.

9. Surveillance Policy for operations as Depository Participant:

- a.** CDSL is providing transactional alerts on Fortnightly basis based on threshold defined by CDSL to the all the Depository Participants including EQUIRUS SECURITIES PRIVATE LIMITED through CDSL report download utility. As per applicable

Communiqués, EQUIRUS SECURITIES PRIVATE LIMITED is reviewing these alerts and taking appropriate actions after carrying out due diligence viz. either disposing off alerts with appropriate reasons/findings recorded or filing Suspicious Transaction Report (STR) with FIU-India in accordance with provisions of PMLA (Maintenance of records) Rules, 2005.

- b. In addition to the same, EQUIRUS SECURITIES PRIVATE LIMITED has framed its Surveillance Policy for Stock Broking operations to generate alerts as per guidance based on following criteria:
- i. Multiple Demat accounts opened with same PAN/mobile number/ email ID/ bank account details/ address. While reviewing BO account details, the details of existing BO shall also be considered.
 - ii. Email/ letters sent to clients on their registered email ID/address which bounces/ returns undelivered.
 - iii. A BO who has submitted modification request for changes in his/her/its demographic details of address, email id, mobile number, bank details, POA holder, Authorized Signatory etc. at least twice in a month.
 - iv. Frequent off-market transfer of securities more than twice in a month without genuine reasons.
 - v. Off-market transactions not commensurate with the income/net-worth of the BO.
 - vi. Pledge transactions not commensurate with the income/net-worth of the BO.
 - vii. High value off-market transfer immediately after modification of either email ID/mobile number/ address without genuine reason.
 - viii. Review of reasons for off-market transfer provided by the BO which appears non-genuine based on either profile of the BO or on account of reason codes, including frequent off-market transfer with reason code gift/donation to unrelated parties and/or with reason code off-market sales.
 - ix. Sudden increase in transaction activity in a newly opened account in a short span of time. An account in which securities balance suddenly reduces to zero and an active account with regular transaction suddenly becomes dormant.
- c. The DP shall review the alerts provided by CDSL on fortnightly basis and shall ensure to process the same as early as possible. In any case, these alerts

will be processed within 30 days from the date of generation of the alert by CDSL.

- x. In case of any delay in disposing off any alerts, reasons for the same shall be recorded.
- d. The DP shall identify suspicious/ manipulative activities undertaken by any client through monitoring of transaction(s)
- e. The DP shall, in case of reporting of any transaction as STR to FIU-India, shall evaluate whether any further action including disassociating with the suspect client(s) and reporting to CDSL/SEBI and/or other Regulatory Authorities.
- f. The DP shall maintain records for such period as is prescribed under PMLA (Maintenance of Records) Rules, 2005, and Securities Contracts (Regulation) Rules, 1957, SEBI (Depository and Participants) Regulations, 1996, DP Operating Instructions and any other directions as may be issued by SEBI/ Stock Exchanges from time to time.

10. Process of disposal of alerts and action:

- a. The designated officials who are tasked to review the alerts on daily basis shall review the same.
- b. If the designated official finds after review and due diligence that the alert is required to be closed, the official shall close the same with appropriate remarks.
- c. If the designated official after due diligence and making such inquiry as such official finds necessarily comes to a conclusion that the alert warrants an action, the official will forward the same with his/her views to the Compliance Officer for his/her approval.
- d. The Compliance Officer, after review of the alerts along with the submitted comments of the designated official, decides to close the alert, he/she shall close it with appropriate remarks. If the Compliance Officer finds that action in respect of such alert is warranted, he/she shall take such actions including filing STR with FIU-India, informing to Stock Exchanges and CDSL and/or discontinue the relationship with the client.
- e. The report of such instances along with adverse observations and details of actions taken shall be submitted to the Stock Exchanges/ CDSL within 7 days from date of identification of such instances.
- f. The records of alerts generated, disposed of as closed and details of action taken wherever applicable shall be maintained with such security measures as would make such records tamper proof and the access is available on to designated officials under the supervision of the Compliance Officer.

11. Obligations of Compliance Officer/ Designated Director and Internal Auditor of the Stock Broking Business and Depository Participant operations:

- a. The surveillance activities of the stock broking operations and that of DP operations shall be conducted under overall supervision of the Compliance Officer of EQUIRUS SECURITIES PRIVATE LIMITED. The policy implemented by EQUIRUS SECURITIES PRIVATE LIMITED in accordance with the provisions of Prevention of Money Laundering Act, 2002 and rules made thereunder as Reporting Entity.
- b. A quarterly MIS shall be put up by the Compliance Officer to the board and the Designated Director giving number of alerts generated during the quarter, number of alerts closed, number of alerts on which action taken with details of action taken and number of alerts pending at the end of the quarter along with reasons for pendency and action plan for closure. The Board as well as the Designated Director shall be appraised of any exception noticed during the disposal of the alerts.
- c. The Designated Director shall be responsible for all surveillance activities carried out by the trading member.
- d. EQUIRUS SECURITIES PRIVATE LIMITED shall submit its surveillance policy to the internal auditor for stock broking operations and internal auditor of DP operations for review and shall satisfy the queries/questions, if any, raised by the internal auditor with respect to the implementation of the surveillance policy, its effectiveness and the alerts generated.

12. Obligation of Quarterly reporting of status of the alerts generated for Stock Broking Operations and Depository Participant Operations :

- a. A quarterly statement providing duly approved status of alerts in respect of stock broking operations on quarterly basis shall be submitted to BSE and NSE in the following format within 15 days after the end of the quarter:
- b. Status of Alerts generated by the Trading Member:

Name of Alert	No. of alerts under process at the beginning of quarter	No. of new alerts generated in the quarter	No. of alerts Verified & Closed in the quarter	No. of alerts referred to Exchange (*)	No. of alerts pending/under process at the end of quarter

c. Details of alerts referred to the Exchange

Sr. No.	Date of Alert	Type of Alert	Brief observation and details of action taken	Date referred to Exchange

d. Details of any major surveillance action taken (other than alerts referred to Exchanges) if any during the quarter

Sr. No.	Brief action taken during the quarter

In case EQUIRUS SECURITIES PRIVATE LIMITED does not have anything to report, a “NIL Report” shall be filed within 15 days from the end of the quarter.

e. A quarterly statement providing duly approved status of alerts in respect of DP operations on quarterly basis shall be submitted to CDSL in the following format within 15 days after the end of the quarter:

f. Status of Alerts generated by the Depository Participant:

Name of Alert	No. of alerts under process at the beginning of quarter	No. of new alerts generated in the quarter	No. of alerts Verified & Closed in the quarter	No. of alerts referred to Exchange (*)	No. of alerts pending/under process at the end of quarter

g. Details of any major surveillance action taken (other than alerts reported to CDSL) if any during the quarter

Sr. No.	Brief action taken during the quarter

In case EQUIRUS SECURITIES PRIVATE LIMITED DP operation does not have anything to report, a “NIL Report” shall be filed within 15 days from the end of the quarter.

13. Effective Date

This policy shall be made effective from 20th September, 2024.

DORMANT ACCOUNT POLICY

ReF: NSE/INSP/43488 Dated 10th February 2020

The circular deals with Dealings between trading members & their clients wherein members were required to frame policy of treatment of inactive accounts and implement the same.

1. **Definition of Inactive Trading accounts:** In case of trading account, the term inactive account refers to such account wherein no trades have been carried out since last 12 (Twelve) months across all Exchanges.
2. **Transaction in Inactive Trading accounts:** The inactive accounts identified based on the above criteria shall be flagged as 'Inactive' in UCC database of all the respective Exchanges and further trading by such client should be allowed only after undertaking sufficient due diligence (including IPV) and obtaining the updated information related to KYC from the concerned Client.
3. **Upload of correct status:** To upload correct status of the client code in the UCC database of the Exchanges prior to the execution of the trades.
4. **Return of Clients assets:** To ensure that all client accounts are settled on monthly or quarterly basis (as per the client preferences) in the manner prescribed from time to time. In case it is not possible to settle the client accounts due to non-availability of client's bank account and demat account details and non-traceability of client, all efforts to trace the clients to settle their funds and securities lying with ESPL is to be done and maintain an audit trail for such efforts made for tracing such clients and settling funds and securities of such clients.
5. **If client is not traced:** If ESPL is unable to trace such clients in spite of all efforts taken, following steps to be taken
 - i) Open one separate Client Bank/Client collateral Demat account and immediately set aside the funds and securities of these clients in such account.
 - ii) Maintain audit trail of UCC wise client funds transferred to/from such bank account and UCC wise / BO ID wise securities transferred to/from such demat account (as the case may be).
 - iii) Submit UCC wise/BO ID wise and fund/securities information of such account to the Exchange on quarterly basis.
 - iv) In case of receipt of any claims from such clients, members are advised to settle the accounts immediately and ensure that the payment/delivery is made to the respective clients only.
5. **Reporting of client Funds & Securities:** It will not be required to upload the details of such inactive clients having NIL balances in their weekly submission of securities holding to the Exchange as prescribed in NSE Circular NSE/INSP/40743 dated April 12, 2019 and NSE/INSP/41711 dated July 25, 2019 and monthly upload of client funds and securities balances to Exchange under Enhanced Supervision prescribed in NSE Circular NSE/INSP/33276 dated September 27, 2016, NSE/ISC/2017/35268 dated July 3, 2017 and NSE/ISC/36817 dated January 24, 2018. However, details of clients having funds or securities balances shall be reported even if their UCC has been flagged as 'Inactive'.