KIFS Broking Private Limited

(A member of National Stock Exchange of India Limited)

ANTI MONTY LAUNDERING POLICY

Version 1.2 (2023)

INDEX

1. **INTRODUCTION TO AML**

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**). The Directives also set out the steps that a registered intermediary or its representatives shall implement to discourage and to identify any money laundering or terrorist financing activities. The relevance and usefulness of these Directives will be kept under review annually 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.

DEFINITION OF MONEY LAUNDERING

Money Laundering is the processing of criminal proceeds to disguise their illegal origin. It is a process by which persons with criminal intent or persons involved in criminal activities attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of illegal funds.

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.

Three most common stages of Money Laundering, as mentioned above are resorted to, by the launderers. The laundered proceeds re-enter the financial system appearing to be normal business funds and Market Intermediaries may unwittingly get exposed to a potential criminal activity while undertaking such normal business transactions. Market Intermediaries are therefore placed with a statutory duty to make a disclosure to the Authorized Officer when knowing or suspecting that any property, in whole or in part, directly or indirectly, representing the proceeds of a predicated offence, or was or is intended to be used in that connection is passing through the Market Intermediaries. Law protects such disclosures, enabling the person with information to be able to disclose the same without any breach of confidentiality. Market Intermediaries likewise need not abstain themselves from providing such information pertaining to its customers.

2. BACKGROUND

This Policy has been framed by M/s. KIFS Broking Private Limited(Hereby referred as "KBPL") in order to comply with the applicable Anti Money Laundering (AML) Standards/ Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and and Pursuant to the recommendations made by the Financial Action Task Force on anti-money laundering standards, SEBI had issued the Guidelines on Anti Money Laundering Standards vide their notification No.ISD/CIR/RR/AML/1/06 dated 18th January 2006, vide Circular No.ISD/CIR/RR/AML/2/06 dated 20th March 2006 vide letter No. ISD/AML/CIR-1/2008 dated December 19, 2008,vide Circular No. ISD/AML/CIR-1/2009 dated September 01, 2009, Vide Circular No. ISD/AML/CIR-2/2009 date October 23,2009, vide Circular CIR/ISD/AML/3/2010 dated December 31, 2010, vide Circular No. ISD/AML/CIR-1/2010 dated February 2010, vide Circular number CIR/MIRSD/11/2014 dated March 12th, 2014, vide Circular SEBI/HO/MIRSD/DOS3/CIR/P/2018/104 dated July 04th, 2018 ,vide Circular No. SEBI/HO/MIRSD/DOP/CIR/P2019/113 dated October 15, 2019 and Circular no. SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 03, 2023 had issued the obligations of the intermediaries registered under Section 12 of SEBI Act, 1992. As per these SEBI guidelines, KSBPL have ensured that proper policy frameworks are put in place as per the Guidelines on Anti Money Laundering Standards notified by SEBI.

Further As per the provisions of the PMLA, every banking company, financial institution (which includes chit fund company, a co-operative bank, a housing finance institution and a non-banking financial company) and 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 , 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 Rs 10 lacs or its equivalent in foreign currency.

- All series of cash transactions integrally connected to each other which have been individually valued below rupees ten 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 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

- 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.

It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' shall also be considered. In case there is a variance in CDD/AML standards prescribed by SEBI and the regulators of the host country, branches/overseas subsidiaries of intermediaries are required to adopt the more stringent requirements of the two.

3. POLICIES AND PROCEDURES TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING

3.1 ESSENTIAL PRINCIPLES:

These 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 consider carefully 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 from time to time.

3.2 OBLIGATION TO ESTABLISH POLICIES AND PROCEDURES:

3.2.1 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.

3.2.2 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

3.2.3 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 the relevant law enforcement authorities, including the 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 KSBPL 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 / Sub-broker. 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.

4. 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 and for that Company take following measures:

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, we shall identify the beneficial owners of the client, 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 15% 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 author 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.

- ✓ **Applicability for foreign investors: D**ealing with foreign investors' may be guided by the clarifications issued vide circular CIR/MIRSD/11/2012 dated September 5, 2012 CIR/ MIRSD/ 07/ 2013 dated September 12, 2013 and SEBI master circulars SEBI/HO/AFD-2/CIR/P/2022/175 date December 19, 2022, 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 our 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.

h. In case of there are suspicion of money laundering or financing of the activities of terriorism or where there are doubt about the adequacy or veracity of previously obtained client identification data , we review the due diligence measure by re-verifying the identity of the client and obtaining information on the purpose and intended nature of the business relationship.

5. 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 not 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.

6. **RISK – BASED APPROACH:**

a. It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the 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 client due diligence 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.

b. Further, low risk provisions shall not be applied 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

c. 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 and
  - 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.

d. RISK MANAGEMENT :

The overall responsibility/implementation and adherence of this KYC/AML policy shall lie with the Compliance team of KIFS Broking Private Limited (KBPL).

The Concurrent / Internal Auditors shall specifically check and verify the application of KYC/AML procedures and comment on the lapses observed in this regard. The reports and compliance in this regard shall also put up before the Board at least at quarterly intervals

7. **CLIENTS OF SPECIALCATEGORY:**

Utmost case 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)/family member or close relative of PEP persons of foreign origin, companies having closed family share holding/beneficial 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.

8. **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 a PEP.

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 obtainedto 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.

9. RELIANCE ON THIRD PARTY FOR CARRYING OUT CLIENT DUE DILIGENCE

KSBPL 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.

Such reliance shall be subject to condition that are specified in rule 9(2) of the PML Rules and further in line with the regulations and circular / guidelines as may be issued by SEBI from time to time. KSBPL shall be ultimately responsible for CDD and

undertaking enhanced due diligence measures, as applicable

10. **RECORD KEEPING REQUIREMENTS& RETENTION OF RECORDS**

Records pertaining to transactions of clients shall be maintained and preserved for a period of five years 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 five years 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. the origin of the funds

ii. the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.

iii. the identity of the person undertaking the transaction;

iv. the destination of the funds;

v. the form of instruction and authority.

System has 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 ten lakh rupees or its equivalent in foreign currency

b. all series of cash transactions integrally connected to each other which have been individually valued below rupees ten 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; for the purpose of suspicious transaction reporting apart from 'transaction integrally connected' 'transaction remotely connected or related' be also considered

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 five years 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.

11. 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.

12. MONITORING OF TRANSACTIONS:

Regular monitoring of transactions of client is vital for ensuring effectiveness of AML procedure and same can be achieved by understanding the normal activities of client. 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/FIUIND/ other relevant Authorities, during audit, inspection or as and when required. These records shall be preserved for a period of five years from the date of transaction with such client. Company shall apply client due diligence measure to existing clients on the basis of materiality and risk and the extent of monitoring shall be aligned with the risk category of the 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. The Compliance Department shall randomly examine a selection of transactions/ clients and comment whether any suspicious transactions are done or not. While monitoring the transactions, company may shift the clients from one category to another depending upon the risk perceived by company

13. **SUSPICIOUS TRANSACTION MONITORING AND REPORTING:**

Company shall maintain records of debits and credits of transactions through various services to the clients, as per their specific instructions. The Rules notified under the PMLA defines a "suspicious transaction" as a transaction whether or not made in cash which, to a person acting in good faith. The list mentioned below is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances

What is a Suspicious Transaction?

- Clients whose identity verification seems difficult or clients appear not to cooperate
- 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 rupees ten lakhs, 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."

Enhance due diligence measures be applied in case of establishing business relationship with clients residing in countries where existence and effectiveness of money laundering control is suspect or which do not or insufficiently apply FATF standard

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.

- There will be continuity in dealing with client as normal until told other wise

and client shall not be told of the report/suspicision

- 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 and 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.

KSBPL is complying the AML (PMLA regulations) by using the existing software of Tech excel. The software provides an alerts related to money laundering activities in the form of suspicious transactions by the clients using the risk based approach. With the help of this system KSBPL monitors, investigates and reports patterns of transactions of a suspicious nature. This enhances due diligence and also ensures compliance with AML regulations and to prevent KSBPL from being used as a medium, intentionally or unintentionally for carrying out money laundering activities.

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://press.un.org/en/content/press-release.

1. The "ISSL (Da'esh) & Al-Quida sanction list , which includes name of individuals and entities associated with the Al-Quaida. The updated ISSL & Al-Quida sancation list is available at : http://www.un.org/securitycouncil/sancations/1267/press-releases

2. The list issued by Unitied Security council resolutions 1718 of designated individuals and entities linked to democratic people's republic of korea http://www.un.org/securitycouncil/sancations/1718/press-releases

3. The list issued by SEBI consequent to list of individuals/entities who are designated as terrorist in pursuance of section 35(1) of UAPA 1967 by the ministry of home affairs as well as orders under section 31(1) and 51A of UAPA

relating to fund, financial assets , economic resources or related services issued by SEBI from time to time.

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 account are linked to any of the entity or individual included in the list.

Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to below authority

14. 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, order dated February 02,2021 and further amendment made vide as Gazzette notification dated June 08, 2021 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.

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 (IS.I), Ministry of Home Affairs, Central [designated] Nodal Officer for the UAPA, at Fax No.011-23092551 and also conveyed over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: jsctcr-mha@gov.in.

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, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, "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. (list of UAPA Nodal Officers is available at the website of Government of India, Ministry of Home Affairs.)

b. 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 (IS.I), 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. Company shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions carried through or attempted in the accounts covered under the list of designated individuals/entities under Section 35 (1) and 51A of UAPA

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 15.3above shall be followed.

14.5 <u>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:</u>

i. 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.

15. **<u>REPORTING TO FIU</u>:**

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) 6th Floor, Tower 2 Jeevan Bharti Building Connaught Place , New Delhi – 110001. Tel-91-11-23314429,23314459,91-11-23319793 (help desk), Email- helpdesk@fiuindia.gov.in as per the schedule given below: (format with relevant details are available at https://fiuindia.gov.in/files/downloads/filing information.html on FIU India website under the section obligation of reporting entity)

Report	Description	DueDate
CTR	All cash transactions of the value of more than Rs.10 Lakhs or its equivalent in foreign currency All series of cash transactions integrally connected to each other which have been valued below Rs.10 Lakhs 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 from the conclusion that the transaction is suspicious
NTR	Non Profit Organization Transaction Report	15th day of the succeeding Month

The 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.

Company shall not put any restrictions on operations in the accounts where an STR has been made. Also company, directors, officers and employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU-IND. This prohibition on tipping off extends not only to the filing of the STR and/ or related information but even before, during and after the submission of an STR. Thus, it will be ensured that there is no tipping off to the client at any level

16. **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.
- Ensure that KSBPL discharges its legal obligation to report suspicious transactions to the concerned authorities.

The Company shall appoint a Principal Officer and communicate the details such as, name, designation and address to the Office of the Director, FIU-IND and update the same whenever there is any change

17. **DESIGNATED DIRECTOR**

"Designated Director" means a person designated by the Board of Directors to ensure over all compliance with the obligations imposed under The Prevention of Money Laundering Act, 2002 and the Rules framed there under, as amended from time to

time, and include the Managing Director or a Whole-time Director duly authorized by the Board of Directors. The Company shall appoint a Designated Director and communicate the details of the Designated Director, such as, name, designation and address to the Office of the Director, FIU-IND and update the same whenever there is any change.

18. **DETAILS OF DESIGNATED DIRECTOR & PRINCIPAL OFFICER**

Name	Mr. Vaibhav Shrivastav	Mr. Nikul Dave
Designation	Principal Officer	Designated Director
Office Address	KIFS Corporate House, 4th Floor, Beside Hotel Planet Landmark, Near Ashok Vatika, Iskon Ambli Road, BRTS, Ambli, Ahmedabad – 380058	
Telephone Number	079-69240000 to 09	
Mobile Number	--------	
Email ID	khandwalallp@gmail.com	

Name and SEBI registration no of entity

Entity Name	**SEBI registration no- stock exchange**
KIFS Broking Private Limited	INZ000244957

19. **SYSTEM AND PROCEDURE FOR HIRING OF EMPLOYEES**

i. The 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 the 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. Key position within organization having regard to the risk of money laundering and terrorist financing will be identified and more stringent norms and care will be applied while selecting and deciding suitability of Candidate

20. **EMPLOYEES TRAINING:**

- Importance of PMLA Act & 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 programs wherever required for new staff, front- line staff, back office staff, compliance staff, risk management staff and staff dealing with new 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.

21. **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.

Note: This policy has been reviewed in terms of SEBI's circular no. SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 03, 2023, SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2023/091 dated June 16, 2023 and SEBI/HO/MIRSD/SEC-FATF/P/CIR/2023/0170 dated October 13, 2023 by Board of Directors KIFS Broking Private Limited during its meeting held on November 8, 2023 and is being circulated to all concerned for compliance of the same.

Risk Categorization

Risk Categorization at the time of account opening:

Category	Particulars
Low Risk	face to face clients, clients forwarded by branches / sub-brokers, authorised person, clients introduced by existing face to face clients
Medium Risk	clients introduced by existing but non-face to face clients
High Risk	Non-resident Clients, Client of Special Categories as mentioned in clause 10 above

Risk Category based on Nature of Business Activity, Trading Turnover etc:-

Risk Category	**CM Segment**	**Derivatives Segment**	**Payment Mechanism**
Low Risk	Average daily turnover < Rs. 50 Lacs or net settlement obligation < Rs. 5 Lacs	Average daily turnover < Rs. 100 Lacs	Regular payment through A/c payee cheque from the Bank A/c already mapped with us
Medium Risk	Average daily turnover > Rs. 50 Lacs but < Rs. 200 Lacs or net settlement obligation > Rs. 5 Lacs but < Rs. 10 lacs	Average daily turnover > Rs. 100 lacs but < Rs. 500 Lacs	Payment through A/c payee cheque from the Bank A/c other than one already mapped with us
High Risk	HNI Clients having average daily turnover of > Rs. 200 Lacs or net settlement obligation of > Rs. 50 lacs	HNI Clients having average daily turnover of > Rs. 500 Lacs	Payment through Banker`s Cheque / Demand Draft / NEFT / RTGS etc.

However, while carrying out transactions for/by the client, RMS Team / department should monitor the trading activity of the client and exercise due diligence to ensure that the trading activity of the client is not disproportionate to the financial status and the track record of the client and shall also take effective measures to mitigate the money laundering and terrorist financing risk with respect to all clients, countries or geographical areas, nature and volume of transactions etc. Accounts department should ensure that payment received from the client is being received in time and through the bank account the details of which are given by the client in KYC form or as may be registered with KBPL and the payment through cash / bearer demand drafts should not be entertained. Further, proper records with audit trail including that of NEFT/RTGS/ECS and other payment modes as may be approved by RBI shall also be maintained and should be made available to competent authorities and self regulatory bodies as and when required.