Guidelines

On

Anti-Money Laundering Standards

Prevention of Money Laundering Act, 2002 (PMLA)

K. M. Global Fin. Serv. Pvt. Ltd.

This policy is applicable for all segments including Cash, Equity Derivatives, Currency derivatives, and all other segments in relation to all exchanges related to K. M. Global Financial Services Pvt Ltd.

I. INTRODUCTION:

Money Laundering is the process by which large amounts of illegally obtained money (from drug trafficking, terrorist activity or other serious crimes) is given the appearance of having originated from a legitimate source. All crimes that produce a financial benefit give rise to money laundering

1. The **Prevention of Money Laundering Act, 2002 (PMLA)** has been brought into force with effect from 1st July 2005. Necessary Notifications / Rules under the said Act have been published in the Gazette of India on 1st July 2005 by the Department of Revenue, Ministry of Finance, Government of India.

2. As per 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 Securities and Exchange Board of India Act, 1992) shall have to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules notified under the PMLA. For the purpose of PMLA, transactions include:

   - 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, such series of transactions within one calendar month.
   - All transactions involving receipts by non-profit organisations of value more than rupees ten lakh, 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.

3. The Anti - Money Laundering Guidelines provides a general background on the subjects of money laundering and terrorist financing in India and provides guidance on the practical implications of the PMLA. The PMLA Guidelines sets out the steps that a registered intermediary and any of its representatives, need to implement to discourage and identify any money laundering or terrorist financing activities.

4. 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 suspect 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.

II.OBJECTIVE OF PMLA:

The main objectives of the PMLA are as follows:

1. To have a proper Customer Due Diligence (CDD) process before registering clients.
2. To monitor/maintain records of all cash transactions of the value of more than Rs.10 lacs.
3. To maintain records of all series of integrally connected cash transactions within one calendar month.
4. To monitor and report suspicious transactions.
5. To discourage and identify money laundering or terrorist financing activities.
6. To take adequate and appropriate measures to follow the spirit of the PMLA.

III. IMPLEMENTATION OF THIS POLICY:

Mr. **Santosh Jha** is the principal officer who is responsible for compliance of the provisions of the PMLA and AML Guidelines acts as a central reference point and plays an active role in identification and assessment of potentially suspicious transactions.

He ensures that K. M. Global Finserv discharges its legal obligations to report suspicious transactions to the concerned authorities.

K. M. Global Finserv being an SEBI registered intermediaries have to comply with spirit of anti money laundering provisions. To comply with PMLA, the following three specific parameters should be observed, which are related to the overall **'Client Due Diligence Process'**:

A. Policy for acceptance of clients;

B. Procedure for identifying the clients;

C. Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR).

Client/Customer Due Diligence (CDD):

For the purpose of CDD, as The Company is dealing mainly with Non- Institutional clients. According to SEBI regulation/rules .:

All other categories of clients viz. Individuals, HUFs, Trusts, Partnership Firms, Companies are considered as non- Institutional Clients.

According to SEBI, all trades done by client should be settled by Clearing Members. Clearing member makes sure that the trades are settled for all retail clients.

In view of above, following steps to be taken to comply with 'Customer Due Diligence'

process before registering as client:

- Obtain basic details for the purpose of the complying with KYC norms prescribed by SEBI (KYC, basically contains basic details of the client like, Name, Address, Occupation, Income level, DP details, Bank Account Details, Details of other Broker where the client is already registered etc).
- List of Directors and authorized person to trade on behalf of client and copy of Board resolution to that effect in case the client is Non Individual.
- Obtain Proof of Identity, Proof of Address after verifying with originals, A recent photograph and such other documents including in respect of his business and financial status of the client
- Intended nature of business relation.
- Custodian details (if any) with whom client trade to be settled.

- Obtain PAN No. (Income Tax number).
- Obtain Risk Disclosure Document duly executed by prospective client as prescribed by SEBI.
- verify identity while carrying out:
- Identify the Beneficial owner and take all reasonable steps to verify his/her idneity
- No anonymous account / fictious account to be opened
- Where the client is a juridical person, it should be verified that any person purpoting to act on behalf of such client is so authorized and verify the identity of that person.

The client/customer due diligence (CDD) measures comprises the following:

- **Client Information & Identity:**
  Before registering client, obtain Antecedent information. Verify independently information submitted by client but not limited to his identity, registered office address, correspondence address, contact details, occupation, Promoters/Directors, source of income, experience in securities market, PAN no, SEBI registration Number, (if any), MAPIN Number (if any) etc. Obtain as much information as can be collected. Generally Retail client are recognize at local level. We shall check the local references for clients identity and other credit details including those mentioned above or we can refer any other reliable, independent source documents, data or information. should be approved by Account Opening Team shall open the Client Account after verifying information collected, registration form along with other supporting documents.

- **Beneficial ownership and control**:
  After completing registration process, client account should be verified by independent employee to check the actual beneficial ownership and control of the particular account. We need to obtain the details with respect to Shareholders, promoters from the non individual clients and wherever possible it has to be verified independently. Also verify the sources of funds for funding the transaction. We also have to take care at the time of settlement regarding nature of transaction, movement/source of transaction, etc. Periodically to ask for clients financial details to determine the genuineness of transaction.

  For this purpose, **"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.

- **Ongoing due diligence and scrutiny:**
  Periodically we need to conduct due diligence and scrutiny of client's transaction and accounts to ensure that transactions are being conducted in knowledge, to find out the risk profile, source of funds, etc. At regular interval, ongoing due diligence and scrutiny need to be conducted 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 organisation's knowledge of the client, its business and risk profile, taking into account, where necessary, the customer's source of funds. We need to periodically update all documents, data or information of all clients and beneficial owners collected under client due diligence process.

A. Policy for acceptance of clients:

Before registering client, we need to identify and verify the following details of the prospective client:

1. Ascertain the category of clients before registration as Client.(i.e. Individual or Non Individual, or other).

2. Obtain all necessary documents for registration. (Photograph, Photo Identity, Proof of Address, copy of PAN, etc). Documents should be verified with original and same to be counter signed by Authorised representative of the organization.

3. Obtain copy of Bank Statement for ascertaining the mode of payment of transaction.

4. Registration of clients to be made on physical presence of the prospective client.

5. Ensure that account should not open in fictitious or benami name.

6. Clients occupation, sources of income.

7. Determine the parameter to categories of client as per risk.

8. Ensure that all details of KYC form should be complete in all respect. Incomplete KYC should not accept by organization.

9. Organization should not register client in case any kind of doubt has been raised by client (i.e. unable to submit required form/proof, any suspicious behavior noticed at the time of registration, etc)

11. Account should not open where organization can not apply Customer Due Diligence/ KYC policies.

12. The client accounts should be scrutinised regularly for determining nature of transaction taken place. In case any suspicious transaction arisen, the account should be freezed or securities/money should not be delivered to client. The suspicious transactions shall be reported to the FIU as well as the respective exchanges or depository where transactions have taken place.

The following safeguards are to be followed while accepting the clients:

a) Security account should not be opened in a fictitious/ benami name or on an anonymous basis.

b) Risk perception of the client need to defined having regard to:

1. Clients' location (registered office address, correspondence addresses and other addresses if applicable);
2. Nature of business activity, trading turnover etc., and
3. Manner of making payment for transactions undertaken.

The parameters of clients into ***low, medium and high risk*** should be classified. Clients of special category (as given below) may be classified as higher risk and higher degree of due diligence and regular update of KYC profile should be performed.

- Customers who are being referred by Director or by management of the Company or by Authorized Person of the Company or by other business associates shall be classified under Low Risk category.

- Rest all customers will be classified under Medium or High Risk category based on facts of the cases. Where a customer is classified under Medium or High Risk category, said accounts should be kept under supervision of Principal Officer.

- Further to above it is also necessary to cross verify the details of prospective customers with the databases of UN or other similar entity. The Company shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to SEBI and FIU-IND.

- 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 Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) needs to be accessed in the United Nations website at http://www.un.org/sc/committees/1267/consolist.shtml

- In addition to above it is also necessary to identify and classify customers under 'Clients of Special Category' (CSC) an illustrative list of 'Clients of Special Category' (CSC) shall be read as under:
    1. Non resident clients,

2. High net-worth clients,
3. Trust, Charities, NGOs and organizations receiving donations,
4. Companies having close family shareholdings or beneficial ownership,
5. Politically exposed persons (PEP). Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.
6. Companies offering foreign exchange offerings,
7. Clients in high risk countries (where existence / effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards, 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,
8. Non face to face clients,
9. Clients with dubious reputation as per public information available etc.

B. <u>Client identification procedure</u>:

<u>To follow the Client Identification procedure we need to follow following factors</u>:

- The 'Know Your Client' (KYC) policy should be strictly observe with respect to the client identification procedure which need to be carried out at different stages i.e. while establishing the Broker- client relationship, while carrying out transactions for the client or when have any doubts regarding the veracity or the adequacy of previously obtained client identification data.
- The client should be identified by using reliable sources including documents / information. Obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.
- Appropriate Risk management systems to be put in place to determine whether the client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic database of PEPS.
- Reasonable measures to be taken to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.
- Each original documents should be seen prior to acceptance of a copy and it is verified and signed by Compliance Officer or personnel as designated by him for such purposes, being without limitation the account opening staff at HO.
- Failure by prospective client to provide satisfactory evidence of identity should be noted and reported to the higher authority within the organization.

- SEBI has prescribed the minimum requirements relating to KYC for certain class of the registered intermediaries from time to time. Taking into account the basic principles enshrined in the KYC norms, internal guidelines should be follow in dealing with clients and legal requirements as per the established practices. Also maintain continuous familiarity and follow-up where it notices inconsistencies in the information provided by the client. The principles enshrined in the PML Act, 2002 as well as the SEBI Act, 1992 should follow, so that organization is aware of the clients on whose behalf it is dealing.

<u>Record keeping</u>:

For the purpose of the record keeping provision, we should ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made thereunder, PML Act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Byelaws and Circulars.

Records to be maintain as are sufficient to permit reconstruction of individual transactions (including the nature of transaction, amounts and types of currencies involved date of the transaction and the parties to the transactions if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.

Should 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, Organization should retain the following information for the accounts of their customers 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:

- the origin of the funds;
- the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;
- the identity of the person undertaking the transaction;
- the destination of the funds;
- the form of instruction and authority.

Organization should ensure that all client and transaction records and information are made available on a timely basis to the competent investigating authorities.

***Retention of Records*:**

The following document retention terms should be observed:

a. All necessary records on transactions, both domestic and international, should be maintained at least for the minimum period of ten years (10) from the date of cessation of the transaction i.e. date of termination of an account or business Relationship.

b. Records on customer identification (e.g. copies or records of official identification documents like PAN card, passports, identity cards, driving licenses or Voter Identity Card or similar documents), account files and business correspondence should also be kept for the ten years (10) from the date of cessation of the transaction.

c. Records of the all trading details of the client needs to be stored for Ten years.

d. Records shall be maintained in hard & soft copies Records should be maintained of all transactions and not merely the transactions that are reported to FIU-IND

In situations where the records relate to on-going investigations or transactions, which have been the subject of a suspicious transaction reporting, they should be retained until it is confirmed that the case has been closed.

Monitoring of transactions:

Regular monitoring of transactions is required for ensuring effectiveness of the Anti Money Laundering procedures.

Special attention require to all complex, unusually large transactions / patterns which appear to have no economic purpose. Internal threshold limits to specify for each class of client accounts and pay special attention to the transaction which exceeds these limits. The background

including all documents, office records and clarifications pertaining to such transactions and their purpose to be examined carefully and findings thereof to be recorded in writing. Such findings, records and related documents to 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 to be preserved for ten years as required under PMLA 2002

It should be ensured that record of transaction is preserved and maintained in terms of section 12 of the PMLA 2002 and that transaction of suspicious nature or any other transaction notified under section 12 of the act is reported to the appropriate law authority. Suspicious transactions should also be regularly reported to the higher authorities / head of the department.

Further, the Compliance Department should randomly examine a selection of transaction undertaken by clients to comment on their nature i.e. whether they are in the suspicious transactions or not.

C. Monitoring Accounts For Suspicious Activity

The company will monitor through the automated means of Back Office Software (specify how suspicious transaction activity would be monitored) for unusual size, volume, pattern or type of transactions. For non automated monitoring, the following kinds of activities are to be mentioned as Red Flags and reported to the Principal Officer.

- The customer exhibits unusual concern about the company compliance with government reporting requirements and the firm's AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents.

- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy.

- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.

- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.

- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.

- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.

- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.

- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the company policies relating to the deposit of cash.

- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the Rs.10,00,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.

- For no apparent reason, the customer insists for multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.

- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.

- The customer requests that a transaction be processed to avoid the company normal documentation requirements.

- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as Z group and T group stocks, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)

- The customer's account shows an unexplained high level of account activity

- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.

- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

When a member of the company detects any red flag he or she will escalate the same to the Principal Officer for further investigation

Broad categories of reason for suspicion and examples of suspicious transactions for an intermediary are

indicated as under:

Identity of Client

- False identification documents
- Identification documents which could not be verified within reasonable time
- Non-face to face client
- Doubt over the real beneficiary of the account
- Accounts opened with names very close to other established business entities

Suspicious Background

- Suspicious background or links with known criminals

Multiple Accounts

- Large number of accounts having a common account holder, introducer or authorized signatory with no rationale
- Unexplained transfers between multiple accounts with no rationale

Activity in Accounts

- Unusual activity compared to past transactions
- Use of different accounts by client alternatively
- Sudden activity in dormant accounts
- Activity inconsistent with what would be expected from declared business
- Account used for circular trading

Nature of Transactions

- Unusual or unjustified complexity
- No economic rationale or bonafide purpose
- Source of funds are doubtful
- Appears to be case of insider trading
- Investment proceeds transferred to a third party
- Transactions reflect likely market manipulations
- Suspicious off market transactions

Value of Transactions

- Value just under the reporting threshold amount in an apparent attempt to avoid reporting
- Large sums being transferred from overseas for making payments
- Inconsistent with the clients apparent financial standing
- Inconsistency in the payment pattern by client
- Block deal which is not at market price or prices appear to be artificially inflated/deflated

IV. Reporting to FIU IND

For Cash Transaction Reporting

- All dealing in Cash that requiring reporting to the FIU IND will be done in the CTR format and in the matter and at intervals as prescribed by the FIU IND

For Suspicious Transactions Reporting

We will make a note of Suspicion Transaction that have not been explained to the satisfaction of the Principal Officer and thereafter report the same to the FIU IND and the required deadlines. This will typically be in cases where we know, suspect, or have reason to suspect :

- the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any the transaction reporting requirement,
- the transaction is designed, whether through structuring or otherwise, to evade the any requirements of PMLA Act and Rules framed thereof
- the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or
- The transaction involves the use of the company to facilitate criminal activity.

We will not base our decision on whether to file a STR solely on whether the transaction falls above a set threshold. We will file a STR and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities.

All STRs will be reported quarterly to the Board of Directors, with a clear reminder of the need to maintain the confidentiality of the STRs

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the PMLA Act and Rules thereof.

V. AML Record Keeping

a. STR Maintenance and Confidentiality

We will hold STRs and any supporting documentation confidential. We will not inform anyone outside of a law enforcement or regulatory agency or securities regulator about a STR. We will refuse any requests for STR information and immediately tell FIU IND of any such request we receive. We will segregate STR filings and copies of supporting documentation from other firm books and records to avoid disclosing STR filings. Our Principal Officer will handle all requests or other requests for STRs.

b. Responsibility for AML Records and SAR Filing

Principal Officer will be responsible to ensure that AML records are maintained properly and that STRs are filed as required

c. Records Required

As part of our AML program, our company will create and maintain STRs and CTRs and relevant documentation on customer identity and verification. We will maintain STRs and their accompanying documentation for at least ten years.

VI. Training Programs

We will develop ongoing employee training under the leadership of the Principal Officer. Our training will occur on at least an annual basis. It will be based on our company size, its customer base, and its resources.

Our training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees' duties; what to do once the risk is identified; what employees' roles are in the company compliance efforts and how to perform them; the company record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PMLA Act.

We will develop training in our company, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos.

We will review our operations to see if certain employees, such as those in compliance, margin, and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

VII. Program to Test AML Program

a. Staffing

The testing of our AML program will be performed by the Statutory Auditors & Compliance officer of the company

b. Evaluation and Reporting

After we have completed the testing, the Auditor staff will report its findings to the Board of Directors. We will address each of the resulting recommendations.

VIII. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the Principal Officer. We will also review the AML performance of supervisors, as part of their annual performance review. The Principal Officer's accounts will be reviewed by the Board of Directors

IX. Confidential Reporting of AML Non-Compliance

Employees will report any violations of the company AML compliance program to the Principal Officer, unless the violations implicate the Principal/Compliance Officer, in which case the employee shall report to the Chairman of the Board, Mr./Ms. Such reports will be confidential, and the employee will suffer no retaliation for making them.

X. **Board of Directors Approval**

We have approved this AML program as reasonably designed to achieve and monitor our company ongoing compliance with the requirements of the PMLA and the implementing regulations under it.

Designated Principal Officer for Compliance with the provision of "Prevention of Money Laundering Act, 2002 [PMLA]:

Mr. Santosh Jha
Surya Mahal, 4th Floor,
5, Burjorji Bharucha Marg,
Fort,
Mumbai- 400001,
Maharashtra

Contact No: Tel: 91-022-22630125
Email: skjha@kmglobal.in