PMLA POLICY

Policy Made on 22nd December, 2008
Reviewed on 30th April 2015

Review of the above PMLA Policy was undertaken on 30th April, 2015 in view of the Circular of SEBI No CIR/MIRSD/1/2014 dated March 12, 2014 for Guidelines on Identification of Beneficial Ownership.

The below mentioned policy on PMLA has been approved by the Board of Directors in their meeting. All the employees are required to follow the same and take due care for its proper implementation.

1. Firm Policy

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.

2. Appointment of Designated Director and his Duties

"Designated Director means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes the Managing Director or a Whole-time Director duly authorized by the Board of Directors"

The firm has designated Shri Vaibhav Varde as the Designated Director of the company to ensure the compliance of the PMLA requirements. Shri Vaibhav Varde is having vast experience in the financial market working.

3. Principal Officer Designation and Duties

The firm has designated Shri Milan Dhanki as the Principal Officer for its Anti-Money Laundering Program, with full responsibility for the firm's AML program. Shri Milan Dhanki is qualified by experience, knowledge and training. The duties of the Principal Officer will include monitoring the firm'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)

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

4. Customer Identification and Verification

At the time of opening an account or executing any transaction with it, the firm will verify and maintain the record of identity and current address or addresses including permanent address or addresses of the client, the nature of business of the client and his financial status as under

Constitution of Client	Proof of Identity	Proof of Address	Others
Individual	PAN Card	Copy of Bank Statement, etc	N.A.
Company	1. PAN Card 2. Certificate of incorporation 3. Memorandum and Articles of Association 4. Resolution of Board of Directors	As above	Proof of Identity of the Directors/Others authorized to trade on behalf of the firm
Partnership Firm	1. PAN Card 2. Registration certificate 3. Partnership deed	As above	Proof of Identity of the Partners/Others authorized to trade on behalf of the firm
Trust	1. PAN Card 2. Registration certificate 3. Trust deed	As above	Proof of Identity of the Trustees/ others authorized to trade on behalf of the trust
AOP/ BOI	• PAN Card • Resolution of the managing body • Documents to collectively establish the legal existence of such an AOP/ BOI	As above	Proof of Identity of the Persons authorized to trade on behalf of the AOP/ BOI

- If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not open the new account.
- All PAN Cards received will be verified form the Income Tax/ NSDL website before the account is opened
- The firm will maintain records of all identification information for ten years after the account has been closed.
- The clients will be categorized into Low Risk & may be changed to Medium and High Risk clients based on the firm policy from time to time.

Clients other than individuals or trusts:

Where the client is a person *other than an individual or trust*, viz., company (unlisted), partnership or unincorporated association/body of individuals, the beneficial owners will be identified 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 25% 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 3 (a) 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 can be exercised through voting rights, agreement, arrangements or in any other manner.

c. Where no natural person is identified under clauses 3 (a) or 3 (b) 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 beneficial owners will be identified, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% 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.

In addition to the above checks the KYC department shall:

(i) Ensure that the identity of the prospective client does not match with a person having known criminal background and that there are no prohibitory orders/sanctions against the prospective client by any enforcement/ regulatory agency.

(ii) Before accepting any person as a client, it must be ensured that such person's name does not appear and is not linked in any way to the individuals and entities listed in the consolidated list of individuals and entities maintained by Security Council Committee established pursuant to United Nations Security Council Resolution 1267 (1999). The consolidated list can be accessed from the UN website at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml and http://www.un.org/sc/committees/1988/list.shtml. All existing accounts should be scrutinized to ensure that no account is held by or linked to any of the individuals or entities included in the aforesaid consolidated list. The Company shall intimate full details of accounts bearing resemblance to any of the individuals/entities in the aforesaid consolidated list to SEBI and FIU-IND.

(iii) It must be ensured that no account, existing or new, bear any resemblance to the designated individuals/entities mentioned in the Schedule to the Government of India (Ministry of Home Affairs – Internal Security-I Division) Order dated August 27, 2009 (as amended) under Unlawful Activities (Prevention) Act, 1967. The updated list of such designated individuals/entities would be communicated by SEBI from time to time. In the event, particulars of any customer (s) match the particulars of designated individuals/entities listed in the said Schedule, the Company shall, within 24 hours, 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 its books to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011- 23092736. Such particulars apart from being sent by post should necessarily be conveyed through e-mail at jsis@nic.in. The company shall also send the particulars of the communication mentioned 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. In case the aforementioned details of any of the customers match the particulars of designated individuals/entities beyond doubt, the Company should prevent designated persons from conducting financial transactions, under intimation 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 should necessarily be conveyed through e-mail at jsis@nic.in. The Company shall also file Suspicious Transactions Report (STR) with FIU-IND covering all transactions in such accounts, carried through or attempted, as per the prescribed format.

(iv) Non Face-to-Face Customers: Company should apply Customer Due Diligence procedures ensuring that the process is equally effective for non face-to-face customers & face-to-face customers. Financial services and products are frequently provided to non face-to-face customers via telephone and electronic facilities including Internet. To mitigate the risks posed by such non face-to-face business, customer due diligence, scrutiny of transactions and trading account should be conducted on an ongoing basis.

(v) All material amendments or alterations to client information (e.g. financial information or standing instructions) should be effected only on receipt of written request from the clients.

(vi) Company shall determine if the existing or potential client is a Politically Exposed Person (PEP) by seeking additional information from clients, accessing publicly available information etc. If the existing/potential client is found to be PEP, approval should be obtained from the Whole-time Director of the Company to admit the PEP as client or to continue the existing business relationship. The Company shall also seek the details of source of funds of clients identified as PEP.

(vii) A copy of client identification program should be forwarded to Director, FIU-IND, New-Delhi.

Risk Profiling of Customers

(i) Risk profiling of all customers should be done based on factors such as customer background, location, nature of business activity or transaction, trading turnover etc. This should be done by the Account Opening Team in consultation with the Principal Officer of the Company. Based on the risk assessment, customers should be grouped into the following three categories –

1. Low Risk
2. Medium Risk
3. High Risk

(ii) The Company shall apply customer due diligence measures to clients on a risk sensitive basis i.e. applicability of customer identification procedures, documentary requirements, ongoing account monitoring, transaction monitoring & risk management will depend on the risk profile of customer. Customers identified as high risk category shall be subjected to enhanced customer due diligence process. Conversely, a simplified due diligence process may be adopted for low risk categories of customers.

(iii) In certain limited circumstances, within the overall framework of the SEBI guidelines, the Company may apply reduced or simplified Customer Due Diligence measures for certain types of customers, products or transactions, taking into account all the risk factors. Any such reduced customer due diligence procedures must be approved by the Principal Officer.

<u>Identification of Clients of Special Category</u>

The company will classify clients as Clients of Special Category and the same shall be subject to periodic review by the Principal Officer

a. Non resident clients
b. High networth clients (Clients having networth above 2.5 Cr)
c. Trust, Charities, NGOs and organizations receiving donations
d. Companies having close family shareholdings or beneficial ownership
e. Politically exposed persons (PEP) of foreign origin

f. Current / Former Head of State, Current or Former Senior High profile politicians and connected persons (immediate family, Close advisors and companies in which such individuals have interest or significant influence)
g. Companies offering foreign exchange offerings
h. Clients in 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.
i. Non face to face clients
j. Clients with dubious reputation as per public information available etc.(Not to accept Entities/Investors Debarred by SEBI/Exchange after verifying PAN in google search)

High degree of due diligence shall be applied in respect of clients of High Risk clients. The process of review of high risk clients will require detailed review at the time of opening of these accounts. Further the transaction of these Clients should be analysed and reviewed. Using various data analystic methods the company would also study the movement in the script in which the clients trade. In case of any modification to the information provided during account opening, the same should be thoroughly analysed and proper care to be taken to avoid any mis-happening. In case any suspicion is found in any activity of such account then the action should be taken to report the same as suspicious to the FIU and other regulators as required in law.

The KYC department should also enquire about the beneficiary information for various non-individual entities and also carry-out the verification process by enquiring for the Proof of Identity & Proof of Address of owners as indicated in the earlier part of the PMLA policy.

All the clients of the company will be continuously reviewed to check whether the client's name not matches with names in any of the following lists:

- SEBI Debarred List

- UNSC

- PEP

- OFAC (Office of Foreign Access and Control given by US Treasury Dept.)

- Such other list that may be specified by the Regulators/Compliance Department from time to time

Further for high risk clients this review will be done on a continuous manner on a weekly / monthly basis as may be decided by the management.

Policy for Acceptance of Clients

The Company has developed customer acceptance policy and procedures which aim to identify the types of customers that are likely to pose a higher than the average risk of money laundering or terrorist financing. Staff should adhere to following safeguards while accepting customers:

- No Trading account should be opened in a fictitious/benami name or on an anonymous basis, or in the name of a suspended/banned entity.
- No Trading account should be opened in the name of any person with criminal background.
- Members of the Company must not establish accounts or relationships involving unregulated money service businesses or unregulated businesses involved in gambling activities.
- No account should be opened if appropriate due diligence measures cannot be applied to a customer for want of verification of documents or on account of non-cooperation of the customer or due to non-reliability of the data/information furnished by the customer.
- In case an account is being opened & operated by an agent on behalf of Principal, it should be specified in what manner the account should be operated,

transaction limits for the operation, additional authority required for transactions exceeding a specified quantity/value and other appropriate details. Further the rights and responsibilities of both the persons (i.e. the agent-client registered with Company).

Reliance on Third Party for Client Due Diligence:

The Client Due Diligence & In-Person verification of the clients will be done by the company staff, however in future if any support / help will be taken from any third party agency then the company will carry out various tests before passing on the responsibility to the third party as the company understands that the Reliance on the third party will be at their own risk and thus will authorize any third party to do the activity only after thorough due diligence from their side before appointing the third party agency.

5. Maintenance of records

The Principal Officer will be responsible for the maintenance for following records

- All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
- All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month;
- All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
- All suspicious transactions whether or not made in cash. Suspicious transaction means a transaction whether or not made in cash which, to a person acting in good faith -
    - gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
    - appears to be made in circumstances of unusual or unjustified complexity; or
    - appears to have no economic rationale or bonafide purpose; or
    - gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism

The records shall contain the following information:

- The nature of the transactions;
- The amount of the transaction and the currency in which it was denominated;
- The date on which the transaction was conducted; and
- The parties to the transaction.

The records will be updated on daily basis, and in any case not later than 5 working days

6. Monitoring Accounts for Suspicious Activity

The following kind of activities are to be mentioned as Red Flags and reported to the Principal Officer.

- The customer exhibits unusual concern about the firm's 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 firm's 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 firm's 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's volume of trading is totally disproportionate to his financial details.
- 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 firm 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

7. 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 firm 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.

8. 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 firm 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 five years.

9. Co-operation with Authorities

(i) The Company and its staff shall cooperate with Anti Money Laundering authorities and shall comply with requirements for reporting any suspicious transactions/activity. However, due regard must be paid to the Company's policy of maintaining customer confidentiality. Confidential information about customers may, therefore, only be given to the authorities when there is a legal obligation to do so.

(ii) The Company and its staff shall strictly ensure that there is no 'tipping-off' to customers about suspicious transaction report being made about their transactions/activities or that the authorities are looking into their transactions/activities. If such information is passed to a customer, it may seriously hamper the enquiry/investigation of the authorities.

(iii) There may be occasions when the authorities ask for a suspect account to be allowed to continue to operate while they progress with their enquiries. In such cases, the Company would cooperate with the authorities, as far as possible, within the bounds of commercial prudence and applicable laws. Senior line management and Principal/Compliance Officer must always be kept aware of such instances.

10. Hiring of Employees:

The company has a sufficient system of screening the employees before their appointment so that they are suitable and competent to perform their duties. The company would also carry out on going employee training programme so that the Employees are adequately trained in AML and CFT procedures as required.

The HR department will also be carrying out the background check of the employee being hired by calling the references provided by the employee or a third party verifier agency to carryout a proper check before employing the employee. The HR department will also try to get the creditability of the employee by talking to the previous employers and get their feedback of the senior / HR department / the department where the employee was working with his past employments.

11. Training Programs for Employees

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 firm's 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 firm's compliance efforts and how to perform them; the firm's 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 firm, 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.

12. Program to Test AML Program

a. Employee

The testing of our AML program will be performed by the Auditors 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.

13. 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

14. Investor Education

The company also intends to take effective steps for Investor Education regarding the PMLA regulations. Accordingly the KYC team of the company intends to Educate the Investor regarding the requirements of PMLA and will also call for various information like Income proof / DP holding / Networth, etc so as to understand the financial position of the client.

15. Confidential Reporting of AML Non-Compliance

Employees will report any violations of the firm's AML compliance program to the Principal Officer, unless the violations implicate the Principal Officer, in which case the employee shall report to the Chairman of the Board, Shri Ramakant Varde. Such reports will be confidential, and the employee will suffer no retaliation for making them.

16. Monitoring and Review of the Company's AML Policy & Procedures

(i) he Company shall undertake regular monitoring of its operations through line management and/or Compliance to check that all businesses are complying with the Company's AML Policy & Procedures as well as local legal and regulatory requirements as prescribed under the PMLA and by SEBI.

(ii) Operational and functional review work shall be undertaken by Compliance and/or Audit functions, as appropriate. Compliance Officer shall liaise with their relevant Audit function counterpart to arrive at appropriate review program and responsibility.

(iii) The level and frequency of monitoring and review work shall be undertaken having regard to materiality and risk in relation to the business and customer base.

17. Procedure for freezing of funds, financial assets or economic resources or related services

In case if any client is found to be guilty under the PMLA provisions then the following procedure to be followed by the Company, will be as under:

1) If the particulars of any of customer/s match the particulars of designated individuals/entities, the Company 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 on their books to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The Company would also convey the information through e-mail at jsis@nic.in.

2) The Company would inform the IS-I Division of MHA so that they may take effective action like informing the State Police and /or the Central Agencies for conducting the verification of the individuals/ entities identified by the registered intermediaries.
3) The Company to provide full support to the appointed agency for conducting of the verification so that the verification gets completed within a period of 5 working days.
4) The Company would not provide any prior notice to the designated individuals/entities.

18. Board of Directors Approval

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

For **M/s R. R. Nabar & Co. Share Brokers Pvt. Ltd.**

Vaibhav Varde
Director

---xxx---