J G Shah Financial Consultants Pvt. Ltd.

PMLA POLICY

VERSION: 4.0
Policy Made on 22nd December, 2008

Reviewed on – 01St July 2025
Reviewed by: Samir S. Shah

Review of the above PMLA Policy was undertaken on 10th February, 23 in view of the Master Circular of SEBI vide Circular **SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 03, 2023** for Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed there under **SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2023/091 dt. June 16, 2023 Amendment to above Guidelines**

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

The company shall appoint a Designated Director, as required under the Rule 2 (ba) of PML. The Designated Director is responsible to discharge the legal obligations to report suspicious transactions to the authorities. In case of any change in the Designated Director, the information regarding the same would be immediately be informed to FIU.

"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 Samir S Shah as the Designated Director of the company to ensure the compliance of the PMLA requirements. Shri Samir S. Shah is having vast experience in the financial market working.

3. Principal Officer Designation and Duties

The company shall appoint a Principal Officer, as required under the Prevention of Money Laundering Act, 2002. The Principal Officer is responsible to discharge the legal obligations to report suspicious transactions to the authorities. The Principal Officer will act as a central reference point in facilitating onward reporting of suspicious transactions and assessment of potentially suspicious transactions. In case of any change in the Principal Officer, the information regarding the same would be immediately be informed to FIU.

The firm has designated Shri Samir S Shah as the Principal Officer for its Anti-Money Laundering Program, with full responsibility for the firm's AML program. Shri Samir S Shah 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 Verify the client's identity using reliable, independent source documents, data or information. Where the client purports to act on behalf of juridical person or individual or trust, the registered intermediary shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person 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 Article of Association 4. Resolution of Board of Directors	As above	Proof of Identity of the Directors / Others authorised 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 / Other authorised 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 / Other authorised to trade on behalf of the trust
AOP / BOI	1. PAN Card 2. Resolution of the managing body 3. Documents to collectively establish	As above	Proof of Identity of the Person authorised to trade on behalf of the AOP /

	the legal existence of such an AOP / BOI		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 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 10% of shares or capital or profits of the juridical person, where the juridical person is a company;

ii) More than 10% of the capital or profits of the juridical person, where the juridical person is a partnership; or

iii) More than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

b. In cases where there exists doubt under clause 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 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: Intermediaries dealing with foreign investors' may be guided by the clarifications issued vide SEBI circulars CIR/MIRSD/11/2012 dated September 5, 2012 and CIR/ MIRSD/ 07/ 2013 dated September 12, 2013, for the purpose of identification of beneficial ownership of the client.

Applicability for client being a non-profit organisation: Every registered intermediary shall register the details of a client on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and the registered intermediary has ended or the account has been closed, whichever is later.

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

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 the entity refers to 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 https://press.un.org/en/content/press-release. The details of the lists are as under:

i. The "ISIL (Da'esh) &Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at: https://www.un.org/securitycouncil/sanctions/1267/press-releases.

ii. The list issued by United Security Council Resolutions 1718 of designated Individuals and Entities linked to Democratic People's Republic of Korea www.un.org/securitycouncil/sanctions/1718/press-releases.

(iii) 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.

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 **jsctrcr-mha@gov.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- 011-23092551 and also convey over telephone on 011- 23092548. The particulars apart from being sent by post should necessarily be conveyed through e-mail at jsctrcr-mha@gov.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 affected 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. The additional norms applicable to PEP as contained in paragraph 14 of the Master Circular shall also be applied to the accounts of the family members or close relatives of PEPs

(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.

Identification of Clients of Special Category

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 centres, 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.

Risk Assessment

i. Registered intermediaries shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its 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 can be accessed at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml and

http://www.un.org/sc/committees/1988/list.shtml).

ii. The risk assessment carried out shall 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.

The Stock Exchanges and registered intermediary shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products. The Stock Exchanges and registered intermediaries shall ensure:

a. To undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and

b. Adoption of a risk based approach to manage and mitigate the risks".

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 - o gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
- o appears to be made in circumstances of unusual or unjustified complexity; or
- o appears to have no economic rationale or bonafide purpose; or
- o 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

5. Record Keeping

Adequate records of all transactions should be maintained in order to support reconstruction of transactions including the amounts, types of currency involved, if any, the origin of funds received into customer's accounts and the beneficiaries of payments out of customers' accounts. These

records should be maintained for a period as required in related act/law after the date of the transaction.

As per Regulations 54 and 66 of the SEBI (Depositories and Participants) Regulations, 2018" & SEBI/HO/MRD2/DDAP/CIR/P/2020/153 dated August 18th, 2020 all necessary records on transactions, both domestic and international, Records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of **eight (8) years** after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later."

The company should record and maintain and preserve the information regarding the transaction as provided in Rule 3 of the PML rules and the information of the same should be maintained for a period of **Five (5) years** or until the trail for the trade.

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.

Records should be maintained of:

- All reports to the authorities and information provided to them;
- The results of any monitoring, which is carried out. These records should be maintained as per requirement in related act/law after closure of the case or such periods as may be required in terms of Company Policies & Procedures or any local regulations, whichever is longer.

All records should be readily retrievable

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

Principal Officer of the Company shall act as a central reference point in facilitating onward reporting of transactions to FIU-IND and for playing an active role in the identification and assessment of potentially suspicious transactions. Principal Officer of the Company shall submit Cash Transaction Reports (CTRs) and Suspicious Transaction Reports (STRs) as prescribed under Rule 3, notified under the PMLA to:

Director, FIU-IND,
Financial Intelligence Unit - India
6th Floor, Tower-2, Jeevan Bharati Building,
Connaught Place, New Delhi-110001, INDIA
Telephone : 91-11-23314429, 23314459
91-11-23319793(Helpdesk) Email:helpdesk@fiuindia.gov.in
(For FINnet and general queries)
ctrcell@fiuindia.gov.in
(For Reporting Entity / Principal Officer registration related queries)
complaints@fiuindia.gov.in
Website: http://fiuindia.gov.in

a) Cash Transaction Reports (CTRs): All cash transactions identified as per clause 7(iii) of this policy should be reported to the FIU-IND in Cash Transaction Reports.

• The CTRs (wherever applicable) for each month should be submitted to FIU-IND by 15th of the succeeding month;

• The Company shall submit the CTRs in electronic format;

• The CD should be accompanied by Summary of Cash Transaction Reports in physical form duly signed by the Principal Officer.

b) Suspicious Transaction Reports (STRs):

• All suspicious transactions shall be reported by the Principal Officer to Director, FIU-IND within 7 working days of establishment of suspicion at the level of Principal Officer. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion.

• The Principal Officer shall submit the STRs in electronic format;

c) The Principal officer will be responsible for timely submission of CTRs & STRs to FIU-IND

d) Utmost confidentiality should be maintained in filling of CTRs and STRs to FIU-IND. The Report may be transmitted by speed/registered post/fax at the notified address

e) No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported.

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.

7. Implementation of Aadhaar:

As per notification given by the MINISTRY OF FINANCE (Department of Revenue) on 1st June, 2017 under Prevention of Money-laundering (Maintenance of Records) Second Amendment Rules, 2017.

The Aadhaar has become mandatory and we have a policy to collect Aadhaar number along with supporting documents from all the clients.

Definitions:

• "Aadhaar number" means an identification number as defined under sub-section (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;
• “Authentication” means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;
• “Resident” means an individual as defined under sub-section (v) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;
• “Identity information” means the information as defined in sub-section (n) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;
• “e – KYC authentication facility” means an authentication facility as defined in Aadhaar (Authentication) Regulations, 2016;
• “Yes/No authentication facility” means an authentication facility as defined in Aadhar (Authentication) Regulations, 2016;
We are complying with important requirements as mentioned in the notification are emphasize as under:

In these there are two types of clients:

• Individual
• Other than Individual i.e. Entities

In case of Individual:

• The client shall submit to us the Aadhaar number issued by the Unique Identification Authority of India;

In case of other than Individual i.e. Entities:

• Client is a Company/Partnership firm/Trust/ Unincorporated association or body of individuals, shall submit to us certified copies of Aadhaar Numbers; Issued to managers, officers or employees in case of company and the person in case of partnership firm/trust/unincorporated association or a body of individuals holding an attorney to transact on behalf of the client entity.

• At the time of receipt of the Aadhaar number under provisions of this rule, shall carry out authentication using either e-KYC authentication facility or Yes/No authentication facility provided by Unique Identification Authority of India (UID).

• If the client does not submit the Aadhaar number, at the time of commencement of an account based relationship with M/S J G Shah Financial Consultants Pvt Ltdthen they submit the same within a period of six months from the date of the commencement of the account based relationship.

• For existing clients already having an account based relationship with reporting entities prior to date of this notification i.e. June 1, 2017, the client shall submit the Aadhaar number by December 31, 2017.

• If client fails to submit the Aadhaar number within the aforesaid time limits the said account shall cease to be operational till the time Aadhaar number is submitted by the client.

• In case the identity information relating to the Aadhaar number submitted by the client does not have current address of the client, the client shall submit an officially valid document to the **M/S J G Shah Financial Consultants Pvt Ltd.**

In view of the Supreme Court judgement dated 26.09.2018 regarding Aadhar Card not being mandatory for registration of clients in the Capital Market, the provision of the above point 17 is not applicable and hence the above point is no longer valid.

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.

As per SEBI Circular dated June 06, 2024 vide the reference number SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2024/78 for guideline on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) / Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed are taken in to account and all the staff member and management will comply with the same.

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

The 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 on a group basis

I. Operational and functional review work shall be undertaken by Compliance and/or Audit functions, yearly. Compliance Officer shall liaise with their relevant Audit function counterpart to arrive at appropriate review program and responsibility.
II. 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 order to ensure expeditious and effective implementation of the provisions of Section 51A of UAPA, Government of India has outlined a procedure through an order dated February 02, 2021 (Annexure 1) for strict compliance. These guidelines have been further amended vide a Gazette Notification dated June 08, 2021 (Annexure 2). A corrigendum dated March 15, 2023 has also been issued in this regard (Annexure 3). The list of Nodal Officers for UAPA is available on the website of MHA".

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.

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

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 broker. Broker 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 CTCR Division of MHA as per the contact details given above within two working days.
II. The Joint Secretary (CTCR), MHA, being the nodal officer for (CTCR) 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 broker. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of CTCR Division shall inform the applicant

The Stock Exchanges and the registered intermediaries shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements

18. Other points The Policy / Documents in relation to CDD will be reviewed once in a year or as per any regulatory changes as an when required and will be presented before the board in the board meeting.

19. Procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 – Directions to stock exchanges and registered intermediaries

The Government of India, Ministry of Finance has issued an order dated January 30, 2023 vide F. No. P-12011/14/2022-ES Cell-DOR ("the Order") detailing the procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 ("WMD Act"). The Order may be accessed by clicking on DoR_Section_12A_WMD.pdf.

In terms of Section 12A of the WMD Act, the Central Government is empowered as under:

"(2) For prevention of financing by any person of any activity which is prohibited under the WMD Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems, the Central Government shall have power to—
(a) Freeze, seize or attach funds or other financial assets or economic resources—

(i) owned or controlled, wholly or jointly, directly or indirectly, by such person; or

(ii) held by or on behalf of, or at the direction of, such person; or

(iii) derived or generated from the funds or other assets owned or controlled, directly or indirectly, by such person;

(b) prohibit any person from making funds, financial assets or economic resources or related services available for the benefit of persons related to any activity which is prohibited under the WMD Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.

(3) The Central Government may exercise its powers under this section through any authority who has been assigned the power under sub-section (1) of section 7."

20. 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 J. G. Shah Financial Consultants Pvt. Ltd

SAMIR SURESHCHANDRA SHAH

Digitally signed by SAMIR SURESHCHANDRA SHAH
DN: c=IN, o=J G SHAH FINANCIAL CONSULTANT P LTD, ou=DIRECTOR, 2.5.4.20=ee7bca904152d3ca1b6a1ee4fc3a3a457d875b5ed01aa586e3b0d03938abb5732, postalCode=400023, st=Maharashtra, serialNumber=78498e5606d6868bfd464938a50b614ae8f75e311bdbb9c5df8f5476087b5441f, cn=SAMIR SURESHCHANDRA SHAH
Date: 2025.11.07 15:08:31 +05'30'

Mr. Samir S. Shah
(Director)