ANTI MONEY LAUNDERING ON STOCK BROKING

FOR

CREATION OF CLIENT AWARENESS

The Prevention Of Money –Laundering Act, 2002 came into effect on 1 July 2005. Section 3 of the Act makes the offense of money-laundering cover those persons or entities who directly or indirectly attempt to indulge or knowingly assist or knowingly are party or are actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property, such person or entity shall be guilty of offense of money-laundering.

Overview & Scope

This Policy describes the documents to be submitted by the client and maintaining of the records by the Organisation. Further it also describes the monitoring process of the Principal Officer in case of any suspicion This policy applies to all the employees of the Organisation including temporary employees, employees on contract etc.

1. PARIM FINSERV 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 & duties of Principal Officer & Designated Partner

The firm has designated Shri. **Paresh Kakadiya** (Managing Partner) as the Principal Officer for its Anti-Money Laundering Program, with full responsibility for the firm's AML program 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.

3. 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	• PAN Card • Certificate of incorporation • Memorandum and Articles of Association • Resolution of Board of Partners	• As above	• Proof of Identity of the Partners/Others authorized to trade on behalf of the firm
Partnership Firm	• PAN Card • Registration certificate • Partnership deed	• As above	• Proof of Identity of the Partners/Others authorized to trade on behalf of the firm
Trust	• PAN Card • Registration certificate • 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

We obtain sufficient information in order to identify persons who beneficially own or control the securities account.

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 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.

4. <u>Risk base Categorisation of Client:</u>

We Classify both the new and existing clients into high, medium or low risk category depending on parameters such as the customer's background, type of business relationship, transactions etc Risk based approach is followed and all client. All client have to submit necessary documents for Deciding Risk Category. Categorisation is based on the documents submitted by client and the due diligence carried out by us.

Further we classified client in Three Categories High Risk, Medium Risk, and Low Risk Following are some point are consider while Categorisation of client

- **High Risk**
  - High risk Client is those Client who not fully satisfied documentation require for Categorisation.
  - Client always have debit Balance in his account without any holding.
  - Delay payment / late payment of fund require for position.
  - Over trading without funds.
  - Poor fanatical background.
  - Nonpayment of dues in account.
- **Medium Risk**
  - Delay payment some time not always.
  - Better fanatical back ground.
  - Good response for debit balance in account.
- **Low Risk**
  - Good DP holding with best fanatical background.
  - Timely payment of funds.
  - Proper document provide for Categorisation of client.

5. **Clients of special category (CSC)**

We also Classified Client according to special category (CSC).

Category include following type

- Non-resident clients
- High net worth clients,
- Trust, Charities, NGOs and organizations receiving donations
- Companies having close family shareholdings or beneficial ownership
- Politically exposed persons (PEP) of foreign origin
- 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)
- Companies offering foreign exchange offerings
- 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.

- ❖ Non face to face clients
- ❖ Clients with dubious reputation as per public information available etc.

6. Risk Assessment

Risk assessment has been done to identify, assess, and take effective measures to mitigate money laundering and terrorist financing risk with respect to clients, countries or geographical areas, nature and volume of transactions, payment method used by clients, etc. It also include any country specific information circulated by Government of India, SEBI etc. from time to time and updated list of individuals and entities who are subjected to sanction measures as required under United Nation's Security Council Resolutions. This assessment will be properly documented, regularly updated and made available to competent authorities and self-regulating bodies as and when required.

7. 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

In terms of Rules made under the PMLA Act, we shall maintain and preserve a record for following time frame:

a. All suspicious transactions whether or not made in cash **for a period of Five years**;
b. 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, account files, business correspondence and all other details as per PMLA guide line **for a period of Five years after the business relationship between client and intermediary has ended or the account has been closed whichever is later** .
c. Suspicious records along with the records of the identity of clients shall be maintained and preserved **for a period of Five years** or as may be in force from time to time from the date of cessation of the transaction between the Client and intermediaries.

8. Monitoring Accounts For Suspicious Activity

The firm 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 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 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

9. 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 Partners, 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.

10. 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 ten years.

11. 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 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. 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

13. Precaution with respect to dormant accounts

All dormant accounts (inactive for six months and more) are made inactive in our system. Hence it is not possible to execute a transaction in dormant accounts. However, a client can re-activate his/her/its dormant account by giving us in writing in prescribed format to activate the account and also stating the reason for keeping the account dormant.

14. 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/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.

15. High standards in hiring policies and training with respect to anti money laundering

The company has adequate screening procedures in place to ensure high standards when hiring employees. The company will identify properly the key position within their own organization structure having regard to the risk of money laundering and terrorist financing and size of their business. The senior management level has been entrusted with the responsibility of complying with the provisions of the ACT and reporting of the suspicious transactions, if any. The employees of the company has been briefed up and trained with the provisions and intentions of the Act putting stress to anti money laundering and anti- terrorist financing.

Hiring of Employees: We shall have adequate screening procedures in place to ensure high standards when hiring employees, having regard to the risk of money laundering and terrorist financing and the size of the business, we ensure that all the employees taking up such key positions are suitable and competent to perform their duties.

Employees' Training: We have an ongoing employee training program conducted by our Principal Officer and Senior Management, Participation of all the Keye Employees in the Seminars conducted by various Regulatory bodies from time to time, so that the members of the staff are adequately trained in AML and CFT procedures.

All the Circulars issued by various Regulatory bodies including that of PMLA, are circulated to all the staff Members and the same are also being discussed in length, in the Training Program'. Training program shall have special emphasis on frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new clients. It is crucial that all those concerned fully understand the rationale behind these directives, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements. 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 pol icy; and the disciplinary consequences (including civil and criminal penalties) f or non-compliance with the PMLA Act.

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,

16. Program to Test AML Program

a. Staffing

The testing of our AML program will be performed by the Statutory 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 Partners. We will address each of the resulting recommendations.

17. Partners 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: **Place: Surat**
Parim Finserv

Paresh Kakadiya
Managing Partner