

**POLICIES AND PROCEDURE FOR PREVENTION OF MONEY LAUNDERING**  
**(Issued as per the requirements of the PMLA Act 2002)**

1. Policy: R L P SECURITIES Pvt. Ltd. had designed this policy of PMLA and effective AML program to prohibit and actively prevent the money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities or flow of illegal money or hiding money to avoid paying taxes. 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.

The policy is prepared taking into consideration the speed and complexity of the transactions, as well as the need for customer due diligence to ensure that undesirable elements are prevented from entering into the system, the policy also ensures compliance with:

- a) THE KYC
- b) RISK BASED MONITORING
- c) TRANSACTION MONITORING
- d) REGULATORY REPORTING
- e) RECORD KEEPING

2. Principal Officer Designation and Duties: The firm has designated Mr. CH. V. A. Varaprasad, Compliance Officer of the Company as the Principal Officer for its Anti-Money Laundering Program. Mr. Varaprasad is a Post Graduate in Commerce from Nagarjuna University, Andhra Pradesh, and is qualified by experience, knowledge and training. The duties of the Principal Officer will include monitoring the firm's compliances with AML obligations and overseeing communication and training the employees on PMLA procedures and to ensure that the employees strictly adhere to the policies laid down on AML activities and PMLA guidelines as per the guidelines set out from time to time and reviewing the same at frequent intervals of time.. 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 company has provided the FIU with contact information of the Principal Officer, including name, title, mailing address, e-mail address, telephone number and facsimile number. The company had been and will be promptly notifying FIU of any change to this information.

3. The policy is prepared taking into consideration the speed and complexity of the transactions, as well as the need for customer due diligence to ensure that undesirable elements are prevented from entering into the system, the policy also ensures compliance with:

- a) THE KYC
- b) RISK BASED MONITORING
- c) TRANSACTION MONITORING
- d) REGULATORY REPORTING
- e) RECORD KEEPING

3 (a). Customer Identification and Verification (The KYC):

- Pre-customer acceptance check

- Comprehensive black list filtering.
- Peer profiling, link analysis and risk based analysis
- Identification of customer with common or similar identity information
- Secondary check on the provision of mandatory information by the customer.

At the time of opening an account or executing any transaction with it, the company 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 by obtaining and verifying the genuineness from the following documents:

<b>Constitution of Client</b>	<b>Proof of Identity</b>	<b>Proof of Address</b>	<b>DP / BANK / OTHER DETAILS</b>
Individual	1. PAN Card	2. Copy of recent Bank Statement, Passport, Voters Id card, Driving License etc.	CMR COPY OF THE DP CANCELED CHQ/ BANK STATEMENT.
Company	3. PAN Card 4. Certificate of incorporation 5. Memorandum and Articles of Association 6. True copy of Certified Board resolution	9. Copy of recent bank statement, Telephone bill, Address proof as obtained from the ROC. etc	CMR COPY OF THE DP CANCELED CHQ/ BANK STATEMENT  Proof of Identity of the Directors / Others authorized to trade on behalf of the firm
Partnership Firm	7. PAN Card 8. Registration certificate 9. Partnership deed	10. Copy of recent Bank statement, Telephone Bill etc	CMR COPY OF THE DP CANCELED CHQ/ BANK STATEMENT Proof of Identity of the Partners/Others authorized to trade on behalf of firm
Trust	11. PAN Card 12. Registration certificate 13. Trust deed	14. As above	CMR COPY OF THE DP CANCELED CHQ/ BANK STATEMENT Proof of Identity of the Trustees/ others authorized to trade on behalf of trust
AOP/ BOI	15. PAN Card 16. Resolution of the managing body 17. Documents to collectively establish the legal existence of such an AOP/ BOI	18. As above	CMR COPY OF THE DP CANCELED CHQ/ BANK STATEMENT Proof of Identity of the Persons authorized to trade on behalf of the AOP/ BOI

All the above documents are verified in original.

IN PERSON VERIFICATION of the clients will be done by the designated employee of our company the verification includes gathering information on financial details and Action taken against clients by SEBI / OTHER AUTHORITIES.

All PAN Cards will be verified from the Income Tax / NSDL website before the account is opened. The company will maintain records of all identification information for ten years after the account has been closed.

Uploading the UCC details to the respective exchange.

It is the policy of the company to reject or refuse the client if the client refuses to co operate in providing the above information or if found suspicious for any reason or customers with common or similar identity information.

Maintenance of records: The Principal Officer will be responsible for the maintenance of the following records

- All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
- The company does not accept any cash transactions in the trading transactions.
- 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;
- 1) 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

### **Transaction Monitoring**

- Analysis of each customer action and transactions against money laundering patterns
- Erase of use, configurable alerts and Scenario management functionality

- Library of alert scenarios, developed after consulting with Industry experts. It should cover typologies varying from large volumes monitoring, off-market transactions, surge in activities etc.
- 'Alert Flood control mechanism' should be available to reduce flood of alerts thereby making the number of alerts, manageable.
- A fully auditable workflow with evidence management to suit the requirements of Brokerage firms.

5. Monitoring Accounts For Suspicious Activity: The company will monitor through the automated means of Back Office Software for unusual size, volume, pattern or type of transactions. For non automated monitoring, 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 maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

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

Broad categories of reason for suspicion and examples of suspicious transactions for an intermediary are indicated as under:

#### Identity of Client

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

#### Suspicious Background

- Suspicious background or links with known criminals

#### Multiple Accounts

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

#### Activity in Accounts

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

#### Nature of Transactions

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

#### Value of Transactions

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

### **Reporting**

- Both MIS reports and Regulatory reports (like CTR and STR) should be supported
- The compliance reports should be generated in the regulatory prescribed format.

#### 6. 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.

#### 7. 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.

8. 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.

9. 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 Directors. We will address each of the resulting recommendations.

10. 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

11. Confidential Reporting of AML Non-Compliance: Employees will report any violations of the company's AML compliance program to the Principal Officer, unless the violations implicate the Compliance Officer, in which case the employee shall report to the Chairman of the Board. Such reports will be confidential, and the employee will suffer no retaliation for making them.

12. 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.