POLICY AND PROCEDURES FOR PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

The Prevention of Money Laundering Act, 2002(PMLA) has been brought into force with effect from 1st July, 2005. As per the provisions of the Act and the SEBI Master Circular No. CIR/ISD/AML/3/2010 dated 31.12.2010, every stock-broker, sub-broker registered under section 12 of the Securities and Exchange Board of India Act, 1992 (SEBI Act, 1992) shall have to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules notified under the PMLA.

Such transaction includes:

- All cash transactions of the value of more than Rs 10 lakhs or its equivalent in foreign currency,
- All series of cash transactions integrally connected to each other which have been valued below Rs 10 lakhs or its equivalent in foreign currency where such series of transactions take place within one calendar month,
- All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into from any non monetary account such as demat account, security account maintained by registered intermediary.

As per the provisions of the Act every Stock Broker and Depository Participant has to develop and implement policies and procedures for prevention of money laundering and terrorist financing.

In line with the said Regulations following **"Policies and Procedures"** has been adopted.

1.1 Customer Due Diligence:

The customer due diligence (CDD) measures comprise the following:

a. To obtain sufficient information in order to identify persons who beneficially own or control securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party should be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

b. To verify the customer's identity using reliable, independent source documents, data or information;

c. To identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the customer and/or the person on whose behalf a transaction is being conducted;

d. To verify the identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c); and

e. To conduct ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the customer, its business and risk profile, taking into account, whose necessary, the customer's source of funds.

f. The clients due diligence process shall be reviewed on a regular basis in order to make the system effective.

1.2 Reliance on Third Party for carrying out Client Due Diligence (CDD)

i. The Company may rely on a third party for the purpose of (a) identification and verification of the identity of a client and (b) determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act.

ii. Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time. Further, it is clarified that the registered intermediary shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

2. Policy for acceptance of clients:

As a measure of customer acceptance policies and procedures that aim to identify the types of customers that are likely to pose a higher than the average risk of money laundering or terrorist financing following safeguards are to be followed while accepting the clients:

a) Only the client account with strong reference should be opened after proper inperson verification. No walk-in clients should be entertained.

b) No account shall be opened in a fictitious / benami name or on an anonymous basis.

c) Factors of risk perception shall be considered by verifying registered office address, correspondence addresses, nature of business activity, trading turnover etc . and manner of making payment for transactions undertaken. The clients shall be classified into low, medium and high risk categories. Clients of special category as mentioned in para. 4 below shall be categorized in higher category requiring higher degree of due diligence and regular update of KYC profile. Further low risk provisions should not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not in fact pose a low risk.

d) It 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.

http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml

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

e) 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.

f) Proper documentation and other information shall be collected in respect of different classes of clients depending on perceived risk and having regard to the requirement to the Prevention of Money Laundering Act 2002, guidelines issued by RBI and SEBI from time to time.

g) No account shall be opened where the Company is unable to apply appropriate clients due diligence measures / KYC policies. The Company shall not continue to do business with a person with suspicious activity. in consultation with relevant authorities.

h) The persons acting for/ on behalf of the clients shall have an authority / consent letter. Adequate verification of a person's authority to act on behalf the client should also be carried out by compliance department.

i) Necessary checks and balance to be put into place before opening an account so as to ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide.

3. Risk-based Approach

It is generally recognized that certain customers may be of a higher or lower risk category depending on circumstances such as the customer's background, type of business relationship or transaction etc. As such, the registered intermediaries should apply each of the

customer due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that the registered intermediaries should adopt an enhanced customer due diligence process for higher risk categories of customers. Conversely, a simplified customer due diligence process may be adopted for lower risk categories of customers. In line with the risk-based approach, the type and amount of identification information and documents that registered intermediaries should obtain necessarily depend on the risk category of a particular customer.

4. Clients of special category (CSC):

Such clients include the following

a. Non resident clients

b. High Networth clients,

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.

The above mentioned list is only illustrative and the Company and principal officer should exercise independent judgment to ascertain whether new clients should be classified as CSC or not.

5. Client identification procedure:

- No walk- in client should be entertained, i.e. it must be introduced by a proper reference of any known person.
- The identity of the client should be properly identified by way of in person verification, PAN card, identity proof, address proof, etc. The in person verification should be done by the employee of the Company authorized for the purpose.
- KYC form should be properly executed in accordance with the requirement of the regulatory authority before becoming the client of the Company.
- Additional care should be taken to determine the clients who are Politically Exposed Person (PEP). Additional information should be collected in case of PEP. The sources of funds of PEP should be identified.
- The client should be identified by the Company by using reliable sources including documents / information. The intermediary should obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.
- The information should be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the Company in compliance with the Guidelines. Each original documents should be seen prior to acceptance of a copy.
- Failure by prospective client to provide satisfactory evidence of identity should be noted and reported to the higher authority within the Company.

6. Record Keeping

6.1 The Company should ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PML Act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

6.2 The Company should maintain such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.

6.3 Should there be any suspected drug related or other laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, registered intermediaries should retain the following information for the accounts of their customers in order to maintain a satisfactory audit trail:

a. the beneficial owner of the account;

b. the volume of the funds flowing through the account; and

c. for selected transactions:

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

6.4 The Company should ensure that all customer and transaction records and information are available on a timely basis to the competent investigating authorities. Where appropriate, they should consider retaining certain records, e.g. customer identification, account files, and business correspondence, for

periods which may exceed that required under the SEBI Act, Rules and Regulations framed there-under PMLA 2002, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.

7. The following information should be maintained in respect of transactions referred to in rule 3 of PMLA rules :

i. The nature of transactions
ii. The amount of transaction and the currency in which it is denominated
iii. The date on which the transaction was conducted
iv. The parties to the transaction.

8. Retention of Records

8.1. The following document retention terms should be followed:

a. All necessary records on transactions, both domestic and international, should be maintained at least for the of 5 years or such other period as prescribed under the relevant Act (PMLA, 2002 as well SEBI Act, 1992) and other legislations, Regulations or exchange bye-laws or circulars.

b. The Company shall maintain and preserve the record of documents evidencing the identity of its clients and beneficial owners (e.g., copies or records of official identification documents like passports, identity cards, driving licenses or similar documents) as well as account files and business correspondence for a period of five years after the business relationship between a client and The Company has ended or the account has been closed, whichever is later

8.2 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.

8.3 Records of information reported to the Director, Financial Intelligence Unit - India (FIU-IND):

The Company shall maintain and preserve the record of information related to transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 & 8 of the PML Rules, for a period of five years from the date of the transaction between the client and the Company.

9. Monitoring of transactions

9.1 Proper monitoring of transactions of the clients should be done thoroughly. Regular monitoring of transactions is vital for ensuring effectiveness of the Anti Money Laundering procedures. Normal activity of the client should be analysed in order to ascertain the deviation in any trades done which is not normal.

9.2 Special attention should be given to all complex, unusually large transactions / patterns which appear to have no economic purpose. Internal parameter should be fixed for all the clients depending on their normal trade practice, income, creditworthiness, risk factor, reference etc. Any breach of parameter should be brought should be analysed properly.

9.3 Transactions done by the clients should be scrutinized and proper clarification should be obtained for the alerts generated for any breach of parameter set by the Company. Alerts should be dropped only after getting proper and satisfactory clarification from the clients / his/ her dealer. In case of alerts for which satisfactory clarification are not received from the clients and which are of suspicious in nature should be reported to the FIU-IND. These records are required to be maintained and preserved for period of five years from the date of transaction between the client and the Company.

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

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

10. Suspicious Transaction Monitoring & Reporting

10.1 **A**ppropriate steps should be taken to enable suspicious transactions to be recognised and have appropriate procedures for reporting suspicious transactions. A list of circumstances which may be in the nature of suspicious transactions is given below. This list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances:

a. Clients whose identity verification seems difficult or clients appears not to cooperate

b. Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;

c. Clients in high-risk jurisdictions or clients introduced by banks or affiliates or other clients based in high risk jurisdictions;

d. Substantial increases in business without apparent cause ;

e. Unusually large cash deposits made by an individual or business;

f. Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;

g. Transfer of investment proceeds to apparently unrelated third parties;

h. Unusual transactions by CSCs and businesses undertaken by shell corporations, offshore banks /financial services, businesses reported to be in the nature of export-import of small items.

10.2 Any suspicion transaction should be immediately notified to the Principal Officer. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it should be ensured that there is continuity in dealing with the client as normal until told otherwise and the client should not be told of the report/suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken.

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

M Prasad & Co Ltd is aware that Under section 51A of Unlawful Activities (Prevention) Act, 1967, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism. The Government is also further empowered to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

12. Reporting to Financial Intelligence Unit- India

The Company should report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address in their prescribed format :

Director, FIU-IND
Financial Intelligence Unit-India
6th Floor, Hotel Samrat
Chanakyapuri
New Delhi- 110021

13. Designation of an officer for reporting of suspicious transactions

The Company has appointed Mr. Rajendra Prasad Bubna, Designated Director as a principal officer. To ensure that the Company properly discharge their legal obligations to report suspicious transactions to the authorities, the Principal Officer would act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions and implementation of SEBI Master Circular no. CIR/ISD/AML/3/2010 dated 31.12.2010.

14. 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. Mr. Bimal Kumar Sultania, Compliance officer 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 intention of the Act putting stress to anti money laundering and anti –terrorist financing. The clients are also educated about the requirement of the PMLA as and when the necessity arises. AML policy will be reviewed on a periodical basis as and when there is a requirement of any modification by the management or the Regulatory body.

15. Designation of Managing Director as Designated Director

The Company has designated Mr. Rajendra Prasad Bubna Managing Director as Designated Director to ensure overall compliance with the obligations imposed under chapter IV of the PMLA Act and the Rules.

For M Prasad & Co Ltd

Compliance Officer