Policy On Prevention Of Money Laundering Act

MANUAL FOR PREVENTION OF MONEY LAUNDERING ACT 2002 (PMLA)

INDEX

PART -I OVER VIEW

1. Introduction

1.1. The Guidelines as outlined below provides a general background on the subject of money laundering and terrorist financing summarizes the main provisions of the applicable anti-money laundering and anti-terrorist financing legislation in India and provides guidance on the practical implications of the Act. The Guidelines also sets out the steps that Branches / Business Associates and any of its representatives, should implement to discourage and identify any money laundering or terrorist financing activities. The relevance and usefulness of these Guidelines will be kept under review and it may be necessary to carryout amendments from time to time.

1.2. These Guidelines are intended for use primarily by our company and its Branches / Business Associates. While it is recognized that a "one-size- fits-all" approach may not be appropriate for the securities industry in India, each Branch / Business Associates should consider the specific nature of its business, organizational structure, type of customers and transactions, etc. when implementing the suggested measures and procedures to ensure that they are effectively applied. The overriding principle is that they should be able to satisfy themselves that the measures taken by them are adequate, appropriate and follow the spirit of these measures and the requirements as enshrined in the Prevention of Money Laundering Act, 2002. (PMLA)

2. Back Ground:

2.1. The Prevention of Money Laundering Act, 2002 has come into effect from 1" July 2005. Necessary Notifications / Rules under the said Act have been published in the Gazette of India on 1st July 2005 by the Department of Revenue, Ministry of Finance, and Government of India.

2.2. As per the provisions of the Act, every banking company, financial institution (which includes chit fund company, a co-operative bank, a housing finance institution and a non-banking financial company) and intermediary (which includes a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992) shall have to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules under the PMLA. Such transactions include:

- ☑ All cash transactions of the value of more than Rs 10 lacs 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 d-mat account, security account maintained by the registered intermediary.

It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' should also be considered.

It is also to be noted that there is NO cash transactions with the Clients of the Company as the Company is primarily into Wealth Services, distribution of financial products including mutual funds.

3. Policies and Procedures to Combat Money Laundering and Terrorist financing

3.1 Essential Principles

3.1.1. These Guidelines have taken into account the requirements of the Prevention of the Money Laundering Act, 2002 as applicable to the intermediaries registered under Section 12 of the SEBI Act. The detailed guidelines in Part II have outlined relevant measures and procedures to guide the Branches / Business Associates in preventing money laundering and terrorist financing. Some of these suggested measures and procedures may not be applicable in every circumstance. Each Branch / Business Associates should consider carefully the specific nature of its business, organizational structure, type of customer and transaction, etc. to satisfy itself that the measures taken by them are adequate and appropriate to follow the spirit of the suggested measures in Part II and the requirements as laid down in the Prevention of Money Laundering Act, 2002.

3.2 Obligation to establish policies and procedures

3.2.1. International initiatives taken to combat drug trafficking, terrorism and other organized and serious crimes have concluded that financial institutions including securities market intermediaries must establish procedures of internal control aimed at preventing and impeding money laundering and terrorist financing. The said obligation on intermediaries has also been obligated under the Prevention of Money Laundering Act, 2002. In order to fulfill these requirements, there is also a need for registered intermediaries to have a system in place for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities.

3.2.2. In light of the above, senior management of a Branch / Business Associates should be fully committed to establishing appropriate policies and procedures for the prevention of money laundering and terrorist financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. The Registered Intermediaries should:

(a) issue a statement of policies and procedures, on a group basis where applicable, for dealing with money laundering and terrorist financing reflecting the current statutory and regulatory requirements;
(b) ensure that the content of these Guidelines are understood by all staff members;
(c) Regularly review the policies and procedures on prevention of money laundering and terrorist financing to ensure their effectiveness. Further in order to ensure effectiveness of policies and procedures, the person doing such a review should be different from the one who has framed such policies and procedures;
(d) adopt customer acceptance policies and procedures which are sensitive to the risk of money laundering and terrorist financing;
(e) undertake customer due diligence ("CDD") measures to an extent that is sensitive to the risk of money laundering and terrorist financing depending on the type of customer, business relationship or transaction; and
(f) develop staff members' awareness and vigilance to guard against money laundering and terrorist financing.

3.2.3. Policies and procedures to combat Money Laundering should cover:

(a) Communication of group policies relating to prevention of money laundering and terrorist financing to all management and relevant staff that handle account information, securities transactions, money and customer records etc. whether in branches, departments or subsidiaries;
(b) Customer acceptance policy and customer due diligence measures, including requirements for proper identification;
(c) Maintenance of records;
(d) Compliance with relevant statutory and regulatory requirements;
(e) Co-operation with the relevant law enforcement authorities, including the timely disclosure of information; and
(f) Role of internal audit or compliance function to ensure compliance with policies, procedures, and controls relating to prevention of money laundering and terrorist financing, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff of their responsibilities in this regard.

PART II – DETAILED OBLIGATIONS

4. WRITTEN ANTI MONEY LAUNDERING PROCEDURES:-

Section 3 of PMLA has defined the "offence of money laundering" as under: "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it is untainted properly shall be guilty of offence of money laundering".

Such procedures should include inter alia, the following specific parameters which are related to the overall Client due Diligence Process':

a. Policy for acceptance of clients
b. Procedure for identifying the clients
c. Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR)
d. Type of Information required to be furnished.Time Limit prescribed by the "FIU-IND"
e. Designated officer for reporting of Suspicious Transactions.
f. Employee Training

5. CLIENT DUE DILIGENCE:-

5.1 Elements of Client Due Diligence Policy

The objective is to ensure that:

a. Obtains sufficient information about to the client in order to identify who is the actual beneficial owner of the securities or on whose behalf transaction is conducted.
b. Verify the customer's identity using reliable, independent source, document, data or information.
c. Conduct on-going due diligence and scrutiny of the account / client to ensure that the transaction conducted are consistent with the client's background / financial status, its activities and risk profile. Every year the financial statements to be taken on record for all corporate clients.

Though it is not possible to know all the details and exact details of the client's background and financial status, it should be our Endeavour to make a genuine attempt towards achieving this. This will be done in two ways:

5.2 Client Acceptance Policy

- ***For New Clients:***

a) Each client should be met in person, before accepting the KYC. The client should be met at the Head Office or any of the branch offices as per mutual convenience of the client and ourselves.
b) Verify the PAN details on the Income Tax website.
c) All documentary proofs given by the client should be verified with original.
d) Documents like latest Income Tax returns, annual accounts, etc. should be obtained for ascertaining the financial status. If required, obtain additional information/document from the client to ascertain his background and financial status.
e) Obtain complete information about the client and ensure that the KYC documents are properly filled up, signed and dated.
f) Ensure that the details mentioned in the KYC matches with the documentary proofs provided and with the general verification done by us.
g) As far as possible, a prospective client can be accepted only if introduced by existing client or associates or known entity. However, in case of walk-in clients, extra steps should be

taken to ascertain the financial and general background of the client.

h) We should not deal with persons who are fictitious / benami / anonymous basis.

i) We should not encourage Client relationship where we are unable to apply appropriate KYC.

j) Risk perception of the client need to defined having regarded to:

- Client's' location (registered office address, correspondence addresses and other addresses if applicable);
- Nature of business activity, tracing turnover etc. and
- Manner of making payment for transactions undertaken.
- The parameters of clients into Clients of special category (as given below) may be classified as higher risk and higher degree of due diligence and regular update of KYC profile should be performed.

For Existing Clients :

Wherever necessary / applicable:

a) Keep updating the financial status of the client by obtaining the latest Income Tax Return, Networth Certificate, Annual Accounts, etc.

b) Update the details of the client like address, contact number, demat details, bank details etc. In case, at any point of time, we are not able to contact the client either at the address or on the phone number, contact the introducer and try to find out alternative contact details.

c) Check whether the client's identity matches 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 local enforcement / regulatory agency. For scrutiny / back ground check of the clients / HNI, websites such as www.watchoutinvestors.com should be referred. Also, Prosecution Database / List of Vanishing Companies available on www.sebi.gov.in and RBI Defaulters Database available on www.cibi1.com should be checked. UNSC, 4.OFAC (Office of foreign Access and Control give by US Treasury department)

d) If a client is found matching with OFAC,UNSC or with SEBI Debarred list we not open the account and immediately informed to Principal Officer/ Designated Director for further action.

e) Scrutinize minutely the records / documents pertaining to clients of special category (like Non-resident clients, High Net worth Clients, Trusts, Charities, NGOs, Companies having close family shareholding, Politically exposed persons, persons of foreign origin, Current/Former Head of State, Current/Former senior high profile politician, Companies offering foreign exchange offerings, etc.) or clients from high-risk countries (like Libya, Pakistan, Afghanistan, etc.) or clients belonging to countries where corruption / fraud is highly prevalent.

f) Review the above details on an going basis to ensure that the transactions being conducted are consistent with our knowledge of customers, its business and risk profile, taking into account, where necessary, the customer's source of funds.

5.3.1. Risk Categorization & Acceptance of Clients through Risk-Based Approach:-

The clients may be of a higher or lower risk category depending on circumstances such as the client's background, type of business relationship or transaction etc. We should apply each of the clients due diligence measures on a risk sensitive basis. We should adopt an enhanced client due diligence process for higher risk categories of client. Conversely, a simplified client due diligence process may be adopted for lower risk categories of client. In line with the risk-based approach, we should obtain type and amount of identification information and documents necessarily dependent on the risk category of a particular client.

5.3.2. Risk Assessment

We shall carry out risk assessment to identify, assess and take effective measures to mitigate any 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/asanctionslist.shtm1 and http://www.un.org/sc/committees/1988/list.shtml).
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.

5.4 Clients of special category (CSC)

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. Typically the clients should be classified as High Risk, Medium Risk, Low Risk as pr below:

Risk	**Indicative List of clients**
High Risk	1. Non Assisted Online clients 2. Non-resident clients (NRI); 3. High Net worth clients (HNI) 4. Trust, Charities, NGOs and organizations receiving donations. 5. Companies having close family shareholdings or Beneficial Ownership. 6. Politically Exposed Persons (PEP) of Foreign Origin 7. 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); 8. Companies offering Foreign Exchange offerings; 9. 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.
Medium Risk	Individual and Non-Individual clients falling under the definition of Speculators, Day Traders and all clients trading in Futures and Options segment
Low Risk	The clients who are not covered in the high & medium risk profile are treated as Low risk Profile client

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

5.5 Client identification procedure (CIP).--

To follow the Client Identification procedure we need to follow following factors:

The 'Know your Client'(KYC) policy should clearly spell out the client identification procedure to be carried out at different stages i.e. while establishing the intermediary — client relationship, while carrying out transactions for the client or when the intermediary has doubts regarding the veracity or the adequacy of previously obtained client identification data.

The client should be identified by using reliable sources including documents / information which is provided by the clients at the time of account opening. We should obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

Appropriate Risk management systems to be put in place to determine whether the client or potential client or the beneficial owner of such client is a politically exposed person.

Such procedures include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic database of PEPS.

Reasonable measures to be taken to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.

The information should be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by us in compliance with the Guidelines. Each original document 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 of the company.

SEBI has prescribed the minimum requirements relating to KYC for certain class of the registered intermediaries from time to time. Taking into account the basic principles enshrined in the KYC norms which have already been prescribed or which may be prescribed by SEBI from time to time, should frame their own internal guidelines based on their experience in dealing with their clients and legal requirements as per the established practices. Further, we should also maintain continuous familiarity and follow-up where it notices inconsistencies in the information provided. The underlying principle should be to follow the principles enshrined in the PML Act, 2002 as well as the SEBI Act, 1992 so that the intermediary is aware of the clients on whose behalf it is dealing.

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.

6. <u>RECORD KEEPING:-</u>

To comply 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.

Maintaining 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.

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.

In terms of rules made under the PMLA Act, Company shall maintain a record of:

a) all cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
b) 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;
c) all cash transaction 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;
d) all suspicious transactions whether or not made in cash;
e) 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; Provided that where it is not possible to verify the identity of the Client at the time of opening an account or executing any transaction, the banking company, financial institution and intermediary, as the case may be, shall verify the identity of the Client within a reasonable time after the account has been opened or the transaction has been executed.

Date of cessation shall mean date of termination of an account or business relationship").

7. INFORMATION TO BE MAINTAINED:-

We should maintain and preserve the following information in respect of transactions referred to in Rule 3 of PML Rules:

a) The nature of the transactions;
b) The amount of the transaction and the currency. in which it is denominated;
c) The date on which the transaction was conducted; and
d) The parties to the transaction

8. RETENTION OF RECORDS:-

Ensure that all customers 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.

The following document retention terms should be observed:

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

(b) Records on customer identification (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 should also be kept for a period of five years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later.".

(c) Where required by the investigating authority, certain records, e.g. client identification, account files, and business correspondence, shall be retained for periods which may exceed those required under the SEBI Act, Rules and Regulations framed there-under PMLA, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.

(d) Suspicious records along with the records of the identity of clients shall be maintained and preserved for a period of five years from the date of cessation of the transaction between the Client and intermediaries.

(e) 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.

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

9. MONITORING OF TRANSACTIONS:-

Regular monitoring of transactions is require for ensuring effectiveness of the Anti Money Laundering procedures.

Special attention require to all complex, unusually large transactions / patterns which appear to have no economic purpose. Internal threshold limits to specify for each class of client accounts and pay special attention to the transaction which exceeds these limits. The background including all documents, office records and clarifications pertaining to such transactions and their purpose to be examined carefully and findings thereof to be recorded in writing. Such findings, records and related documents to be made available to auditors and also to SEBI/Stock Exchanges/FIU-IND/Other relevant authorities, during audit, inspection or as and when required. These records to be preserved for five years as required under PMLA 2002

It should be ensured that 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. Further, the Compliance Department 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:-

For the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' need to be considered

Suspicious transactions" means a transaction relating to deposit, withdrawal, exchange or transfer of hinds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical whether or not made in cash which to a person acting in good faith —

(a) gives rise to a reasonable ground of suspicion that it may involve the proceeds of an offense specified in the schedule to the act regardless of the value involved ; or

(b) Appears to be made in circumstances of unusual or unjustified complexity or

(c) Appears to have no economic rationale or bonafide purpose. or

(d) Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;

All the Branches/business associates shall report all Suspicious Transaction to Compliance Department immediately on observation.

On basis of the alerts generated as above / on basis of continuous monitoring, Compliance department has to furnish the information of the suspicious transactions to the Principal Officer immediately.

Whether a particular transaction is suspicious or not will depend upon the background details of the client, details of the transactions and other facts and circumstances. Followings are the circumstance, which may be in the nature of suspicious transactions: -

a) Clients whose identity verification seems difficult or clients appears not to co-operate;

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 volume without apparent cause;

e) High exposures taken by client as compared to income levels informed by clients.

f) Unusual transactions by "Client of Special category (CSCs)" and businesses undertaken by offshore banks /financial services, businesses reported to be in the nature of export-import of small items.

Any suspicion transaction need to be notified immediately to the Money Laundering Control Officer or designated 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. The Principal Officer, compliance, risk and surveillance team should have timely access to customer identification data, CDD information transaction records and other relevant information. The Principal Officer shall report to the Board of Directors and to the Director Operations jointly. Further the employees shall keep the fact of furnishing information in respect of transactions referred to above strictly confidential 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.

Clients of high risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards published by FATF .on its website (wwww.fatf-gafi.org),which are categorized as "clients of Special

Category" to be subjected to appropriate counter measures. Measures which include enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or systematic reporting of financial transactions, and application of enhanced due diligence at the time of expanding business relationships with the identified country or persons in that country to be implemented.

Also steps to be taken to independently access and consider other publicy available information.

It should be ensured that irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA 2002 , STR is filed if there are reasonable grounds to believe that the transactions involve proceeds of crime.

a. Due Date

The Principal Officer has to furnish the information of the suspicious transactions to Director, FIU-IND within 7 working days of establishment of suspicion at the level of Principal Officer

Format

Suspicious Transaction Report in manual format has to be filed in following forms:

Description of Form	Information
Suspicious Transaction Report for an Business Associates	Details of suspicious transactions
Annexure A- Individual Detail Sheet for an Business Associates	Identification details of individual
Annexure B- Legal Person/ Entity Detail Sheet for an Business Associates (Non Individual)	Identification details of legal person /entity
Annexure C- Account Detail Sheet for an Business Associates	Details of account and transactions

11. LIST OF DESIGNATED INDIVIDUALS/ ENTITIES:-

Maintain updated list of individuals / entities which are subject to various sanctions / measures pursuant to United Nations Security Council Resolutions (UNSCR), available from the URL http://www.un.org/sc/committees/1267/consolist.shtml. (Referred to as designated individual / entities) in electronic form. Ensure before opening any new account that the name of the proposed customer does not appear in the list of designated individuals / entities.

12. PROCEDURE FOR FREEZING OF FUNDS, FINANCIAL ASSETS OR ECONOMIC RESOURCES OR RELATED SERVICES

Section 51A, of the Unlawful Activities (Prevention) Act, 1967 (UAPA), relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government has issued an Order dated August 27, 2009 detailing the procedure for the implementation of Section 51A of the UAPA. Under the aforementioned Section, 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.

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

http://www.un.org/sc/committees/1267/conso1ist.shtml. We will ensure that accounts are not opened in the name of anyone whose name appears in said list. We shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to SEBI and FIU-IND.

13. REPORTING (DISCLOSURE) OF SUSPICIOUS ACTIVITY

The 'Principal Officer' shall report the information relating to suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address as may modified by the SEBI from time to time:

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

Time limit prescribed for information to FIU -IND:

Rule 8 of the rules notified by notification No.9/2005 (as amended by Notification No.15/2005 and 4/2007) prescribes time limit for furnishing information to the Director, FIU-IND

The time limit for furnishing information about cash transactions and integrally connected cash transactions to Director, FIU-IND is 15th day of the succeeding month.

All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions should be furnished to the Director, FIU-IND not later than seven working days from the date of occurrence of such transactions.

All suspicious transactions have to be furnished to the Director, FIU-IND not later than seven working days on being satisfied that the transactions is suspicious.

No restrictions should be put on operations in the accounts where an STR has been made. All directors, officers and employees (permanent and temporary) are prohibited from disclosing ("tipping off') the fact that a STR or related information is being reported or provided to the FIU-IND.

14. DESIGNATION OF AN OFFICER FOR REPORTING OF SUSPICIOUS TRANSACTIONS:-

The Company has designated Mr.Karthik KS, Compliance Officer to ensure overall compliance with the obligations imposed under chapter IV of the PMLA Act and the Rules. The Compliance Officer will ensure filing of necessary reports with the Financial Intelligence Unit (FIU —IND). The company has appointed for Trading & DP as the Principal Officer. The Principal officer appointed 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 shall have access to and be able to report to senior management at the next reporting level or the Board of Directors. Names, designation and addresses (including email addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-FIU. As a matter of principle, it is advisable that the 'Principal Officer' is of a sufficiently senior position and is able to discharge the functions with independence and authority.

Review Policy:

We are reviewing the PMLA policy as and when there are any changes introduced by any statutory authority or as and when it is found necessary to change on account of business needs and Risk Management policy.

The policy reviewed by Principal Officer & Compliance Officer and placed the changes in policy before the Board at the meeting first held after such changes are introduced and the same is communicated to all departmental heads and associate persons via email and a copy of the reviewed policy is also made available on our website.

Miscellaneous

All employees shall ensure compliance with this policy. It shall be the duty of every Employee/ Business Associate of the Company to cooperate with and provide timely disclosure and information to any inspecting authority (either internal or external) including any relevance law enforcement authorities with regard to implementation of this policy.

In addition to this policy all directives issued by SEBI/ Exchanges or any other regulatory authority shall be strictly adhered to.