SHCIL SERVICES LIMITED

ANTI MONEY LAUNDERING POLICY

INDEX

1.BACKGROUND

The Prevention of Money Laundering Act, 2002 (PMLA) has been brought into force with effect from 1st July 2005 and it provides for Anti-money Laundering and Anti-terrorist Financing measures to be taken in India and the rules framed there under provides guidance on the practical implementation of the provisions laid down in the Act. The Director appointed by Financial Intelligence Unit-INDIA (FIU-IND) has been conferred with exclusive and concurrent powers under relevant sections of the Act to implement its provisions. The Act imposes an obligation on banking companies, financial institutions and intermediaries associated with the securities market and registered with the Securities and Exchange Board of India (SEBI) under section 12 of SEBI Act, 1992 to adhere to client opening procedures and maintain records of such transactions as prescribed under the PMLA and Rules notified thereunder. The stock brokers fall under the category of intermediaries under section 12 of SEBI Act, 1992, and hence the provisions of PMLA are also applicable to all the sock brokers. Establishment of Anti-money Laundering programs by Market Intermediaries are one of the central recommendations of the Financial Action Task Force (FATF).

SEBI has issued necessary directives from time to time vide its circulars covering issues related to Know Your client (KYC) norms, Anti Money Laundering (AML), Client Due Diligence (CDD) and Combating Financing of Terrorism (CFT). This policy document is based on the SEBI's master circular on PMLA bearing reference no. ISD/AML/CIR-1/2010 dated February 12, 2010 and subsequent circulars bearing reference no.CIR/ISD/AML/2/2010 dated June 14, 2010 and CIR/ISD/AML/3/2010 dated December 31, 2010, which consolidates requirements/obligations to be fulfilled by all the registered intermediaries, SEBI Circular No. CIR/MIRSD/1/2014 dated March 12, 2014 and SEBI/HO/MIRSD/DOS3/CIR/P/2018/104 dated July 4, 2018.

This policy will be subject to changes in order to incorporate further directives that SEBI may give vide its circulars on PMLA, from time to time.

- Banking Company
- Financial Institution
- Intermediary (which includes a stock broker, sub-broker, share transfer agent, portfolio manager, other intermediaries associated with securities market and registered under section 12 of the SEBI Act,1992)

The aforesaid entities 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 > Rs 10 Lac or its equivalent in foreign currency
- All integrally connected series of cash transactions < Rs 10 Lac or its equivalent in foreign currency within one calendar month.
- All suspicious transactions, whether or not made in cash and including inter-alia credits or debits from any non-monetary account such as demat account, security account maintained by SSL.

2. DEFINITION OF MONEY LAUNDERING

Money Laundering is the processing of criminal proceeds to disguise their illegal origin. It is a process by which persons with criminal intent or persons involved in criminal activities attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of illegal funds.

Although money laundering is a complex process, it generally follows three stages:

Placement is the initial stage in which money from criminal activities is placed in financial institutions. One of the most common methods of placement is structuring— breaking up currency transactions into portions that fall below the reporting threshold for the specific purpose of avoiding reporting or recordkeeping requirements.

Layering is the process of conducting a complex series of financial transactions, with the purpose of hiding the origin of money from criminal activity and

hindering any attempt to trace the funds. This stage can consist of multiple securities trades, purchases of financial products such as life insurance or annuities, cash transfers, currency exchanges, or purchases of legitimate businesses.

Integration is the final stage in the re-injection of the laundered proceeds back into the economy in such a way that they re-enter the financial system as normal business funds. Banks and financial intermediaries are vulnerable from the Money Laundering point of view since criminal proceeds can enter banks in the form of large cash deposits.

Three most common stages of Money Laundering, as mentioned above are resorted to, by the launderers. The laundered proceeds re-enter the financial system appearing to be normal business funds and Market Intermediaries may unwittingly get exposed to a potential criminal activity while undertaking such normal business transactions. Market Intermediaries are therefore placed with a statutory duty to make a disclosure to the Authorized Officer when knowing or suspecting that any property, in whole or in part, directly or indirectly, representing the proceeds of a predicated offence, or was or is intended to be used in that connection is passing through the Market Intermediaries. Law protects such disclosures, enabling the person with information to be able to disclose the same without any breach of confidentiality. Market Intermediaries likewise need not abstain themselves from providing such information pertaining to its customers.

Consequences of Money Laundering

Finances Terrorism:

Money laundering provides terrorists with funds to carry out their activities

Undermines rule of law and governance:

Rule of Law is a precondition for economic development – Clear and certain rules applicable for all.

Affects macro economy:

Money launderers put money into unproductive assets to avoid detection.

Affects the integrity of the financial system:

Financial system advancing criminal purposes undermines the function and integrity of the financial system.

Reduces Revenue and Control:

Money laundering diminishes government tax revenue and weakens government control over the economy.

Suspicious Transaction

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
- Appears to be made in circumstances of unusual or unjustified complexity
- Appears to have no economic rationale or *bona-fide* purpose
- Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism
- Identity verification or address details seems difficult or found to be forged / false Asset management services where the source of the funds is not clear or not in keeping with apparent standing /business activity
- Substantial increases in business without apparent cause
- Unusual & Unexplained large value of transaction
- Transfer of large sums of money to or from overseas locations
- Unusual & Unexplained activity in dormant accounts

3. FINANCIAL INTELLIGENCE UNIT (FIU)-INDIA

The Government of India has set up FINANCIAL INTELLIGENCE UNIT (FIU)-INDIA on November 18, 2004 as an independent body to report directly to the Economic Intelligence Council (EIC) headed by Finance Minister.

FIU-IND has been established as the central national Agency responsible for receiving, processing, analyzing and disseminating information related to suspect financial transactions. FIU-IND is also responsible for co-ordinating and stretching efforts of national and international intelligence and enforcement agencies in pursuing the global efforts against money laundering and related crimes.

4. ANTI MONEY LAUNDERING PROGRAM (AML)

The objective of having an AML Program is to have in place adequate policy, practice and procedure that help to prevent money-laundering activities. Such procedures would include the following:

- Appointment of Principal Officer.
- Client Due Diligence is the main part of the policy and includes following:
    - Client Acceptance Policy
    - Client Identification Procedure
- Transaction monitoring to identify & report Suspicious Transactions (STR). The rules for identifying and reporting suspicious transactions would be mentioned separately in an AML procedure document.
- Record keeping & retention of records
- Co-operating with law enforcement agencies in their efforts to trace the money laundering transactions and persons involved in such activities
- On-going training to the employees to ensure strict adherence to Customer
- Due diligence requirements

- Reports to Financial Intelligence Unit-India (FIU-IND)

SSL has implemented the AML (PMLA regulations) Software procured from TSS Consultancy. This Anti Money Laundering System provides a means to prevent or report money laundering activities in the form of suspicious transactions by the clients using the risk based approach. With the help of this system SSL monitors, investigates and reports patterns of transactions of a suspicious nature. This enhances due diligence and also ensures compliance with AML regulations.

These procedures and standards would assist in knowing and understanding the activities of its existing and prospective clients and to prevent SHCIL Services Limited (SSL) from being used as a medium, intentionally or unintentionally for carrying out money laundering activities. The chapters ahead detail the AML program adopted by the company.

5. APPOINTMENT OF PRINCIPAL OFFICER

SSL will identify an official from amongst the staff members to act as Principal Officer under the provisions of PMLA.

The Managing Director shall be the competent authority for identifying the Principal and Alternate Officers. The details of appointment of the Principal

Officer will be intimated to FIU-IND immediately.

RESPONSIBILITIES OF PRINCIPAL OFFICER:

The Principal Officer will ensure that:

1. The PMLA Guidelines and the Board approved PMLA policy is implemented effectively by the company.

2. The identification and assessment of potentially suspicious transactions are done on the regular basis.
3. SSL reports the suspicious transactions to the concerned authorities within the specific time as per the PMLA policy.
4. SSL is regularly updated regarding any changes/ additions/ modifications in PMLA provisions obtained through circulars etc.

5. SSL responds promptly to any request for information, including KYC related information, made by the regulators, FIU-IND and other statutory authorities.
6. Any other responsibilities assigned by Managing Director or any other official authorized by Managing Director with respect to the implementation of PMLA guidelines issued by SEBI / Regulator / Government Authority from time to time.

6. CONSTITUTION OF PMLA COMMITTEE

The Principal Officer shall constitute a PMLA (Prevention of Money Laundering Act) Committee to facilitate operational convenience. This committee shall have representation from Operations and from the risk management and legal departments from support functions.

The Committee shall have a Chairman appointed by the Principal Officer whose role should include the following:

- Convening of PMLA Committee meetings as and when required
- Presenting the views of the PMLA Committee to the Principal Officer for his decision making.

The Principal Officer may change the constitution of the PMLA Committee whenever required.

7. CLIENT DUE DILIGENCE:

7.1 CLIENT ACCEPTANCE POLICY:

Considering the potential threat of usage of the financial services by a money launderer, it is essential to make reasonable efforts to determine the true identity of clients. SSL has to put in place effective procedures to obtain requisite details for proper identification of new customers.

1. All the clients shall require to disclose the details of designated bank account and designated demat account in the Account Opening Form. All the pay-in /pay–out of funds/ securities shall be routed through designated bank / demat account only. No cash/DD shall be accepted.
2. ALL KYC Documentations and Procedures shall be followed at the time of account opening and no account shall be opened where SSL is unable to apply appropriate CDD measures/ KYC policies. This may be applicable in cases where it is not possible to ascertain the identity of the client, or the information provided to the SSL is suspected to be non genuine or there is perceived non cooperation of the client in providing full and complete information

3. The submission of all documents required under this policy shall be pre- requisite for account opening for all clients. Incomplete application including incomplete documentation will be rejected. SSL will follow the industry standard for implementing client identification procedure.

4. Since SSL has no direct clients other than Institutional clients, the authorized official/employees of sub broker (Stock Holding Corporation of India Ltd, which is also holding Company of SSL is major sub broker of SSL) shall personally verify the photograph of the client affixed on the Account Opening Form (AOF) and the proof of identity documents with the person concerned. A stamp of "Identity Verified In Person" must be affixed (as a proof of In Person Verification) on the AOF against the photograph of the client & on the proof of identity documents. The authorized official of the SHCIL who has done in- person verification and verified the documents with original should also sign on the AOF and ID proof.

5. Each original document shall be seen prior to acceptance of a copy. Stamp of "documents verified with originals" must be affixed along with the signature of the authorized person.
6. In case of any discrepancy or non-provision of information by the client, SHCIL/other sub broker shall seek necessary clarification from the applicant and activate the account only when the discrepancy is resolved or the deficiency is fulfilled. E.g. cases where names mentioned on the AOF and that on the PAN Card do not match etc.
7. Verify the customer's identity using reliable, independent source documents, data or information by following procedure:

   The PAN Card details should be verified with the name(s) appearing on the website of the Income Tax Department, http://incometaxindiaefiling.gov.in/challan/enterpanforchallan.jsp?pAction=Post and /or TIN website of NSDL e-governance. In case the name(s) do not match or the PAN Card details are not present in the PAN Card database, SHCIL/other sub broker should seek necessary clarification from the applicant(s) and activate the account only when the discrepancy is resolved.
8. Reasonable precaution to be taken that no account is opened in a fictitious/ benami name or on an anonymous basis.
9. The applicant shall be required to disclose his/ her financial status and occupation details as required by PMLA.
10. Account Opening Form (AOF) shall be strictly as prescribed by Security Exchange Board of India.
11. If the applicant has completed KYC procedure with any KYC Registration Agency (KRA), in-person-verification shall be adequate.
12. In case of clients other than an Individual or trust, viz., company, partnership firm or un incorporated association / body of individuals, is shall be mandatory for such clients to disclose the beneficial ownership in them. In particular following

information shall be obtained from such clients:

- Shareholding pattern of the company having more than 25% holding in the share capital
- Profit sharing ratio of partners having more than 15% share in profit
- Any juridical person having more than 15% of the property or capital in an unincorporated association or body of individuals

13. In case the client is trust, the following information shall be obtained from such clients:
    - List of the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
14. With regard to client with a dubious reputation, SSL will obtain the information from various other legitimate sources like

    http://www.sebi.gov.in,
    http://www.sebi.gov.in/pmd/debarredco1.html,
    http://www.sebi.sebi.gov.in/pmd/debardirector1.html,
    http://www.sebi.gov.in/cis_prosecutiondata.html,
    http://www.sebi.gov.in/cis/noncisdata.html,
    http://www. watchoutinvestors. com/default2a.asp,
    UN Security Council website - http:// www.un.org/en/sc/,
    OFAC website - http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx etc.

15. SSL shall comply with the provisions of the Government order dated August 27, 2009 for implementation of Section 51A of the Unlawful Activities Prevention Act, 1967.

7.2 CLIENT IDENTIFICATION PROCESS:

Guidelines on information needed to be obtained to identify BO.

In case of Natural Persons

Dealer shall obtain sufficient data to verify identity of the customer, his address, his location and his recent photograph. It is required to find out whether customer is acting on behalf of another person as intermediary.

Dealer shall ask for receipt of satisfactory evidence of the identity of the intermediary and person on whose behalf intermediary is acting and nature of arrangement.

In case of legal / juridical persons

Dealer shall verify legal status through the documents submitted.

Dealer shall understand the ownership and control structure of such legal person and ascertain who are the natural persons in ultimate control of the legal person. Dealer shall identify such beneficial owners who control the legal person. Even the authorised signatories of the legal persons shall be ascertained and identified.

Also following precautions will have to be taken by SSL in order to ascertain that accounts are not misused by the clients or by any third parties for money laundering activities:

1. SSL will obtain information about the client as per the requirement mentioned in the AOF for the different categories of clients.
2. Verify client's identity
3. SSL will register clients as per SEBI / BSE / NSE/ MSE / MCX / ICEX guidelines and it will develop appropriate reporting system to monitor client's trades.
4. SSL shall periodically update all documents, data or information of all clients and beneficial owners collected under CDD process provided the client provides the information.
5. SSL shall implement the procedure to determine whether the potential client is a politically exposed person. PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country

   e.g. Heads of States or of Governments, senior politicians, senior government, judicial or military officers, senior executives of the state owned corporations,

important political party officials etc. In case of PEPs enhanced CDD measures shall be applicable as noted in the procedure It is required to obtain senior management approval for establishing/ continuing business relationship with PEPs.

7.3 PARAMETERS TO IDENTIFY THE LEVEL OF RISK OF CLIENTS

At the time of acceptance: HNI, Trusts, PEPs and NRIs clients are considered as high risk clients.

During the course of Trading:

High Risk Clients: The clients whose single trade value in a day is more than Rs.5 lac are considered as high risk clients.

Medium Risk Clients: The clients whose single trade value in a day is less then Rs.5 lac and more than Rs. 2 lac are considered as Medium risk clients.

Low Risk Clients: The clients whose single trade value in a day is less then Rs.2 lac are considered as Low risk clients.

The transactions carried out by high and medium risk clients shall be monitored with special attention commensurate with the income declared by clients.

In addition to above, special emphasis shall be on identification of client/BO who might be political exposed person (PEPs) from the various sources available in public domain and availing the services of the specialized agencies. Further, approval from the senior management shall be obtained for establishing business relationships with PEPs in case of a new client and where a client has been accepted and the client or beneficial owner is subsequently found to be a

PEP, approval from senior management shall be obtained to continue the business relationship with such client.

The aforesaid parameters shall be revised from time to time.

8. RECRUITMENT & TRAINING OF EMPLOYEES

SSL shall ensure adequate screening procedures at the time of hiring its staff. It shall also ensure that the employees dealing with PMLA requirements are suitable

and competent to perform their duties.

SSL will conduct PMLA awareness program for its existing employees to ensure that they are aware of their obligations under the provisions of PMLA. SSL will ensure that the new staff recruited by them is also given initial PMLA awareness training.
SSL will also arrange for periodical refresher training to the staff to keep them updated on new developments and to communicate any changes in the policies, procedures etc.

SSL shall make periodic updates to the AML Policy on the intranet for creating awareness on PMLA among the employees.

9. Investor Education:

SSL shall take measures to educate the Investor about the requirements, importance and necessity of the PMLA including any amendments, circulars and notifications through new letters, personal meetings etc, Once the AML/ CFT measures are implemented investor is required to provide the sensitive information like documents evidencing his source of funds, his income tax returns, bank statements etc. Clients are likely to voice their apprehensions about the motive and purpose of collecting such information by SSL. In such case Dealer / back office staff members are required to make the investor aware that these requirements are arising from the AML/CFT framework. The Dealer / back office staff should prepare specific literature & pamphlets so as to educate the investor / customer about the objectives of the AML / CFT Programme.

The letters are also required to be sent to the clients on the updates of the said programme.

10. RECORD KEEPING & RETENTION OF RECORDS

PMLA stipulates that records pertaining to all cash transactions greater than Rs. 10 lakhs, all integrally connected series of transactions are maintained for a period of 5

years. PMLA further stipulates that all relevant documents like Account Opening Forms and their supporting documents, business correspondence and all instructions for operating the account given by client or its duly registered Power of Attorney should be maintained at least for a minimum period of 5 years after the account is closed. In cases where the records relate to on-going investigations or transaction reporting, they should be retained until it is confirmed that the case has been closed.

In view of this, SSL shall maintain the records in terms of the provisions of PMLA. The retention period shall be modified on receiving appropriate instructions from any regulatory authority like SEBI, FIU-IND or any other statutory authority.

11. MONITORING OF TRANSACTIONS

In addition to the parameters laid down in clause no 7.3, SSL shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

The Compliance Department shall ensure adherence to the KYC policies and procedures. Internal Auditors shall specifically check and verify the application of KYC procedures and comment on the lapses if any observed in this regard. All staff members shall be provided training on Anti Money Laundering. The focus of training shall be different for frontline staff, compliance staff and staff dealing with new customers.

The Compliance Department shall randomly examine a selection of transactions/ clients and comment whether any suspicious transactions are done or not. While monitoring the transactions, SSL may shift the clients from one category to another depending upon the risk perceived by SSL.

12. IDENTIFYING OF SUSPICIOUS TRANSACTIONS

SSL shall maintain records of debits and credits of transactions through various services to the clients, as per their specific instructions.

The Rules notified under the PMLA defines a "suspicious transaction" as a transaction whether or not made in cash which, to a person acting in good faith-

a) Give rise to reasonable ground of suspicion that it may involve proceeds of crime

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

c) Appears to have no economic rationale or bona fide purpose.

13. REPORTING OF SUSPICIOUS TRANSACTIONS:

The staff of the operations department concerned shall monitor all transactions executed by clients and report to the PMLA Committee any transaction that appears to be of suspicious nature. Also system generates file of suspicious transactions based on few set parameters and informs CR staff to download such data for further investigation. The Principal Officer shall analyze and examine such data and then decide if any transaction listed therein warrants a closer inspection or not. He shall maintain the records of all such data received from authority and record the action taken against any client for suspicious transactions.

In case the Principal Officer comes across any transaction that appear to be of suspicious nature, he shall also submit the report of such transactions directly to The Director, FIU-IND in the prescribed format, within seven working days of establishment of suspicion.

SSL shall not put any restriction on operation in the accounts of any client where an STR has been made and the same has been reported to FIU-IND. SSL shall also be prohibited from disclosing the same to the client for whom the STRs have been reported to FIU-IND. However, in exceptional circumstances consent may not be given to continue to operate the account, and transaction may be suspended.

Provisions regarding requirement of implementing the Government order dated August 27, 2009 for implementation of Section 51A of the Unlawful Activities Prevention Act.

PMLA software also updates the list of individuals / entities linked to Al – Qaida. As such before opening any new trading account it is ensured that name of the proposed customer does not appear in the said list. Also existing trading accounts are scanned to ensure that no account is linked to any of the entities or individuals included in the list. As such, SSL strictly follows the procedure laid down in the UAPA order dated August 27, 2009.

SSL shall time to time abide and comply with the circulars and guidelines issued by the Regulators/Exchanges and other law enforcement agencies.

14. REVIEW OF POLICY

The aforesaid AML policy shall be reviewed periodically with regard to testing its adequacy to meet the compliance requirements of PMLA 2002 and relevant circulars issued by Regulatory/ Statutory bodies.

****

SHCIL SERVICES LIMITED

PROCEDURE
OF
ANTI MONEY LAUNDERING

The Customer Due Diligence Process for PML :

- Acceptance of Clients
- Client Identification Procedure
- Suspicious Transactions identification & reporting

Clients Acceptance Procedure

All the clients shall require to disclose the details of designated bank account and designated demat account in the Account Opening Form. All the pay-in /pay–out of funds/ securities shall be routed through designated bank / demat account only. No cash/DD shall be accepted.

Each client should be met in person: Since SSL has no direct clients other then Institutional clients, the authorized official/employees of Stock Holding Corporation of India Limited (SHCIL) which is a sub broker of SSL shall personally verify the photograph of the client affixed on the Account Opening Form [AOF) and the proof of identity documents with the person concerned. A stamp of "Identity Verified in Person" must be affixed (as a proof of In Person Verification) on the AOF against the photograph of the client & on the proof of identity documents. The authorized official of the SHCIL who has done in- person verification and verified the documents with original should also sign on the AOF and ID proof.

Accepts clients on whom we are able to apply appropriate KYC procedures: *Obtain* completes information from the client. It should be ensured that the initial forms taken by the clients are filled completely. All photocopies submitted by the client are verified against the original documents without any exception. Ensure that the 'Know Your Client' guidelines are followed without any exception. All supporting documents as specified by Securities and Exchange Board of India (SEBI) and Exchanges are obtained and verified

Do not accept clients having identity that matches the persons known to have criminal background: Check whether the client's identify matches with any person having any known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement/regulatory agency worldwide.

Do not compromise on submission of mandatory information/ documents: Client's account should be opened only on receipt of mandatory information along with authentic supporting documents as per the regulatory guidelines. Do not open

the accounts where the client refuses to provide information/documents and we should have sufficient reason to reject the client towards this reluctance

Clients Identification Procedure

We have a mechanism in place to establish identity of the client along with firm proof of address to prevent opening of any account which is fictitious / benami / anonymous in nature.

Documents which can be relied upon:

- *PAN Card*: PAN card is mandatory and is most reliable document as only one card is issued to an individual and we can independently check its genuineness through IT website.

- *IDENTITY Proof*: PAN Card itself can serve as proof of identity. However, in case PAN card carries an old photograph of the holder, which does not match current facial features of the client, we should take other identity proof in form of Voter's Identity card, Passport, Ration Card or any Government/PSU/Bank issued photo identity card.

- *ADDRESS Proof*: For valid address proof we can rely on Voter's Identity Card, Passport, Bank Statement, Ration card and latest Electricity/telephone bill in the name of the client.

Documents to be obtained as part of customer identification procedure for new clients:

a. In case of individuals, one copy of the following documents have to be obtained

- As PAN is mandatory, verify its genuineness with IT website and cross verify the PAN card copy with the original. [Please put "verified with original" stamp as proof of verification]

- Other proofs for identity are Voter's Identity card, Passport, Ration Card or any Government/PSU/Bank issued photo identity card or any other document prescribed by the regulatory authorities.

- Address proof in the form of Voter's Identity Card, Passport, Bank Statement, Ration card and latest Electricity/telephone bill in the name of the client or any other document prescribed by the regulatory authorities.

b. In case of Corporates, one certified copy of the following documents must be obtained:

Copy of the Registration/Incorporation Certificate

- Copy of the Memorandum & Articles of the Association
- Copy of the PAN card and the Director Index No. (DIN)
- Copy of the latest audited Annual Statements of the corporate client
- Latest Net worth Certificate
- Latest Income Tax return filed.
- Board Resolution for appointment of the Authorized Person who will operate the account.
- Proof of address and identity of Authorized Person

C. In case of Partnership firm, one certified copy of the following must be obtained:

Registration certificate

- Partnership Deed
- PAN card of partners
- Authorization letter for the person authorized to open and operate the account
- Proof of identity and address of the authorized person.
- Annual statement/returns of the partnership firm

d. In case of a Trust, one certified copy of the following must be obtained:

- Registration certificate
- Trust Deed
- PAN card
- Authorization letter for the entity authorized to act on their behalf

- Officially valid documents like PAN card, voters ID, passport, etc of person(s) authorized to transact on behalf of the Trust.

f. In case of an NRI account - Repatriable/non-repatriable, the following documents are required:

- Copy of the PIS permission issued by the bank
- Copy of the passport
- Copy of PAN card
- Proof of overseas address and Indian address
- Copy of the bank statement
- Copy of the CMR for demat account
- If the account is handled through a mandate holder, copy of the valid PoA/mandate

8. Risk Profiling of the Client

We should accept the clients based on the risk they are likely to pose. The aim is to identify clients who are likely to pose a higher than the average risk of money laundering or terrorist financing. For this purpose, we need to classify the clients as Low risk, medium risk and high risk clients. By classifying the clients, we will be in a better position to apply appropriate customer due diligence process. That is, for high risk client we have to apply higher degree of due diligence.

In order to achieve this objective, all clients of the branch should be classified in the following category viz:

At the time of acceptance: HNI, Trusts, PEPs and NRIs clients are considered as high risk clients.

During the course of Trading:

High Risk Clients: The clients whose single trade value in a day is more than Rs.5 lac are considered as high risk clients.

Medium Risk Clients: The clients whose single trade value in a day is less then Rs.5 lac and more than Rs. 2 lac are considered as Medium risk clients.

Low Risk Clients: The clients whose single trade value in a day is less then Rs.2 lac are considered as Low risk clients.

The transactions carried out by high and medium risk clients shall be monitored with special attention in commensurate with the income declared by clients.

The aforesaid parameters shall be revised from time to time

9. Suspicious Transactions

The staff of the operations department concerned shall monitor all transactions executed by clients and report to the PMLA Committee any transaction that appears to be of suspicious nature. Also system generates file of suspicious transactions based on few set parameters and informs CR staff to download such data for further investigation. The Principal Officer shall analyze and examine such data and then decide if any transaction listed therein warrants a closer inspection or not. He shall maintain the records of all such data received from authority and record the action taken against any client for suspicious transactions.

In case the Principal Officer comes across any transaction that appear to be of suspicious nature, he shall also submit the report of such transactions directly to The Director, FIU-IND in the prescribed format, within seven working days of establishment of suspicion.

****