

## **Indbank Merchant Banking Services Limited**

### **Policy Guidelines on Know Your Client (KYC) and Prevention of Anti Money Laundering (AML)**

#### **Preamble**

#### **Guidelines issued by SEBI**

The Prevention of Money Laundering Act, 2002 (PMLA) was brought into force with effect from 1<sup>st</sup> July 2005. Necessary Notifications / Rules under the said Act were published in the Gazette of India on July 01, 2005. Subsequently, SEBI issued necessary guidelines vide circular no. ISD/CIR/RR/AML/1/06 dated January 18, 2006 to all securities market intermediaries as registered under Section 12 of the SEBI Act, 1992. These guidelines were issued in the context of the recommendations made by the Financial Action Task Force (FATF) on anti-money laundering standards. The same was communicated to branches for their information, guidance and implementation.

#### **Anti Money Laundering Standards**

Money laundering is the process whereby proceeds of crimes such as drug trafficking, smuggling, etc. are converted into legitimate money. The criminals attempt to hide and disguise the true origin and ownership of the proceeds of criminal activities, thereby avoiding prosecution, conviction and confiscation of criminal funds. Thus money laundering is involvement in any transaction or series of transactions that seeks to conceal or disguise the nature or source of proceeds derived from illegal activities.

#### **Objectives of Prevention of Money Laundering**

The Anti Money Laundering Policy is to establish governing policies and standards to protect financial intermediaries from being used to launder money. The policy objectives are:

- i. To protect the financial institutions including intermediaries from being used for money laundering
- ii. To adhere to the statutory guidelines with regard to 'Know Your Customer' (KYC) policies and procedures
- iii. To take appropriate action, once suspicious activity is detected and make report to the designated authorities in accordance with the applicable law/laid down procedures
- iv. To comply with applicable laws as well as norms stipulated by the statutory authorities like NSE / BSE / SEBI etc.

As per the provision of the Act, all banking company, financial institution and intermediary (which includes a stock broker, sub-broker, DP, share transfer agent etc.) 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:

- a) All cash transactions of value of more than Rs.10.00 lakhs or its equivalent in foreign currency.
- b) All series of cash transactions integrally connected to each other which have been valued below Rs.10.00 lakhs or its equivalent in foreign currency where such series of transactions take place within one calendar month.
- c) All suspicious transactions whether or not made in cash and including, inter-alia, credit or debits into from any non monetary account such as de-mat account, security account maintained by the registered intermediary.

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

### ***KYC Guidelines - A Tool to Prevent Money Laundering***

Know Your Customer (KYC) guidelines are important tools to ensure that the financial system is not used for laundering proceeds of criminal activities. KYC norms/guidelines play a very important role in preventing money laundering.

To meet the regulatory requirements and to guide the field level functionaries of the companies, it was decided to frame comprehensive Policy guidelines on Prevention of Anti Money Laundering. Accordingly this Policy guidelines are prepared for information, guidance and implementation.

#### **Company's detailed KYC Policy:**

##### **Who is a Customer?**

For the purpose of KYC policy, a 'Customer' is beneficiary of transactions conducted by professional intermediaries, such as Stock Brokers etc., as permitted under the law.

##### **Objectives**

The main objective of KYC guidelines is ***to prevent the company from being used, intentionally or unintentionally, by criminal elements for money laundering activities.***

Know Your Customer is the principle on which the company operates to avoid the pitfalls of operational, legal and reputation risks and consequential losses by scrupulously adhering to the various procedures laid down for opening and conduct of accounts.

The KYC guidelines *go beyond* merely establishing the identity of the person. The due diligence expected under KYC involves going in to the *purpose and reasons for opening the account*, anticipated turnover in the account, *source of wealth (net worth)* of the person opening the account and sources of funds flowing into the account. Thus, this is not a responsibility, which ends with the opening of the account. *Ongoing monitoring* is an essential element of effective KYC procedures.

**Other objectives in stipulating KYC guidelines are:**

- To minimize frauds
- To check misappropriations
- To weed out undesirable customers
- To Prevent Money Laundering
- To avoid opening of accounts in anonymous or benami / fictitious names and addresses

**Need for Policies and Procedures to Combat Money Laundering and Terrorist financing**

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.

**Prevention of Money Laundering Policy of the company contains the following aspects:**

- a) Policies and procedures, on a group basis wherever applicable, for dealing with money laundering and terrorist financing reflecting the current statutory and regulatory requirements;
- (b) The Policy is drafted in such a way that the content of these Guidelines are understood by all staff members;

- (c) The Policy laid down is subject to review by the competent authority from time to time as per the guidelines issued by the statutory authorities from time to time.
- (d) Customer acceptance policies and procedures which are sensitive to the risk of money laundering and terrorist financing;
- (e) 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.

**The Policy and procedure to combat Money laundering covers:**

- 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 Registered Office;
- 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.

**Salient Features of Revised Policy**

In order to achieve the objectives of Anti Money Laundering guidelines by the statutory authorities, under the overall "Client Due Diligence Process" the following three key elements have been made.

- i. Policy for acceptance of clients (**Appendix I**)
- ii. Procedure for identifying the clients (**Appendix II**)
- iii. Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR) (**Appendix III**)

**The salient features of the company's revised KYC policy and Anti Money Laundering Standards are summarised below:**

- a. **Policy for acceptance of Clients** has been framed as part of KYC policy
- b. Parameters of risk perception for customers have been defined based on which customers are to be categorized
- c. Preparation of a profile for each customer based on the risk categorisation
- d. Fixing of threshold limit for each account (based on risk perception) to have effective monitoring
- e. **Procedure for identifying clients** have been spelt out for different types of customers and the documents/information to be obtained have been dealt in detail
- f. **Guidelines for Transaction monitoring and Suspicious Transactions Reporting (STR).**
- h. Appointment of Principal Officer for the company for monitoring and reporting of identified / suspicious transactions and sharing information as required under the law.

#### **Obligation to Maintain Secrecy of Information Received**

Branches/**Terminals** should treat the information collected from the customer for the purpose of opening of account as confidential and not divulge any details thereof either for cross selling or for any other purposes. Branches/**Terminals** shall therefore, ensure that information sought from the customer under KYC norms

- i. is relevant to the perceived risk
- ii. is **not** intrusive
- iii. is in conformity with the guidelines issued by the company from time to time in this regard.

#### **Record Keeping**

As per the master circular issued by SEBI on prevention of Money Laundering the registered intermediary 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.

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, we 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.

The company shall ensure that all customer and transaction records and information are available on a timely basis to the competent investigating authorities. Wherever 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.

More specifically, the following records, as prescribed under Rule 3, notified under the Prevention of Money Laundering Act (PMLA), 2002, are to be maintained by service branch where all the operations of the company is centralized, for a period of **TEN YEARS**.

- (i) All cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
- (ii) All series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceed rupees ten lakh;
- (iii) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
- (iv) All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

**Information to be Maintained:**

The following in formations are to be maintained as referred to in Rule 3 of PMLA Rules:

- I. the nature of the transactions;
- II. the amount of the transaction and the currency in which it denominated;
- III. the date on which the transaction was conducted; and
- IV. the parties to the transaction.

**The following are the document retention terms:**

- (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), account files and business correspondence should also be kept for the same period.
- (c) 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.

**KYC for the existing accounts**

The revised guidelines will apply to all new customers and to the existing customers on the basis of materiality and risk. All the existing accounts of companies, trusts, and other institutions shall be subjected to minimum KYC standards which would establish the identity of the natural/legal person and those of the 'beneficial owners'. However, transactions in existing accounts should be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the Customer Due Diligence measures.

**Non co-operation, Non submission of documents/data/information by customer**

In respect of existing accounts, where the branch/terminal is not able to apply KYC norms especially in monitoring of transactions due to non co-operation by the customer, or non reliability of the data/information furnished to the company, branch/terminal may stop the operations forthwith.

**Principal Officer**

Vice President & Company Secretary or such other officer nominated by the President of the company shall be the authority to ensure the effective implementation of Company's KYC policy and Anti Money Laundering measures by branches. He shall explicitly allocate duties and responsibilities for ensuring that

policies and procedures are managed effectively and that there is full commitment and compliance to an effective KYC programme in respect of both existing and prospective accounts. It should cover proper management oversight, systems and controls and other related matters. Compliance of instructions / guidelines issued by SEBI/NSE/BSE from time to time is to be reported to all branches by the Principal Officer

Branch/Terminal In Charges/Service Branch Head shall be responsible for ensuring that company's policies and procedures are implemented in letter and spirit and that there is full commitment and compliance to an effective KYC programme in respect of both existing and prospective deposit accounts.

### **Training of Staff**

It is crucial that all the operating and management staff fully understand the need for strict adherence to KYC norms and Anti Money Laundering measures. Training requirements will have different focuses for frontline staff, compliance staff and staff dealing with new customers so that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

### **Role of Internal Auditor:**

Internal audit should cover in their report as to whether the policies and guidelines framed by the company in line with the SEBI guidelines are being followed or not. The report shall also cover the compliance requirement of relevant statutory and regulatory authorities and Co-operation with the relevant law enforcement authorities including the timely disclosure of information.

**Appendix - I**  
**Policy for acceptance of clients**

**Our Company's Policy for acceptance of clients is based on the following principles:**

- a) No account is opened in a fictitious / benami name or on an anonymous basis.
- b) No account would be opened without client classification with regard Risk Perception
- c) Documentation requirement and other information to be collected in respect of
- d) 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 Stock Exchanges, Depositories, RBI and SEBI from time to time.
- e) No account shall be opened where the branch/terminal is unable to apply Appropriate clients due diligence measures / KYC policies.
- f) In respect of Power of Attorney accounts adequate verifications of the persons authority to open and operate the account shall be carried out before opening the account.
- g) Due verification would be made 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.

**Categorisation of customers**

As regards categorisation based on risk perception, customers are to be categorised into three\_levels as under:

- Low Risk Customers**
- Medium Risk Customers**
- High Risk Customers**

**Low Risk Customers**

The following category of clients will fall under this category:

Individuals [other than High Net Worth and entities opening Stock broking and/or Demat *account* whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, are to be categorised as low risk customers

Illustrative examples of low risk customers are:

- i. Salaried employees whose salary structures are well defined, Pensioners

- ii. People belonging to lower economic strata of the society whose accounts show small balances and low turnover
- iii. Individuals whose annual income from known sources does not exceed Rs. 10 lakhs

### **Medium Risk Customers**

Customers that are likely to pose a slightly more than average risk to the company are to be categorized as medium risk customers (Category II).

Illustrative examples are:

- I High Networth Individuals. For this purpose an individual is considered as high net worth whose annual income from known sources is above Rs.10.00 lakhs and up to Rs.25 Lakhs.
- ii. NRI Customers
- iii. Corporate Customers
- iv. Accounts of individuals operated by a Mandate or Power of Attorney Holder
- v. Companies (both Private and Public), with *annual turnover up to Rs. 5 Crores*
- vi. Accounts of Trusts / HUF

Under this category, branches/terminals should apply enhanced Customer Due Diligence (CDD) while opening accounts. Branches/Terminals shall call for *additional* information and documentary evidence, besides the normal documents prescribed for low risk customers

### **High Risk Customers:**

Customers that are likely to pose a high degree of risk to the company are to be categorized as high risk customers (Category III). Examples of this type of customers are:

High Net worth Individuals, with annual income from known sources is above Rs.25 Lakhs.

- a. Companies (both Private and Public) having close family shareholding or beneficial ownership
- d. Trusts, Charities, NGOs and organisations receiving donations
- c. Politically Exposed Persons (PEPs) of foreign origin
- d. Non-face to face customers
- e. Clients with dubious reputation as per public information available
- f. Companies offering foreign exchange offerings
- g. 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)

- 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. All other accounts/entities that could not be categorised under Low and/or Medium Risk

Branches/Terminals should apply *intensive* Customer Due Diligence (CDD) while opening accounts of High Risk Customers especially those for whom the sources of funds are not clear.

**Non co-operation, Non submission of documents / data / information by customer**

Where the branch/terminal is unable to apply appropriate customer due diligence measures i.e. branch/terminal is unable to verify the identity and/or obtain documents required as per the risk categorisation due to non co-operation of the customer or non reliability of the data/information furnished to the company, the branch/terminal may take a decision **not to open** the account.

## Appendix II

### Client Identification Procedures

1. To achieve the objectives of the KYC framework that is
  - (i) to ensure appropriate customer identification and
  - (ii) to monitor transactions of a suspicious nature

Branches/Terminals should obtain all information necessary to establish the identity/legal existence of each new customer, based preferably on disclosures by customers themselves.

2. Client identification means identifying the customer and verifying his/her/its identity by using reliable, independent source documents, data or information. Client Identification Procedure is to be carried out at different stages i.e. while opening the account; carrying out a financial transaction or when the branch/terminal has a doubt about the authenticity/ veracity or the adequacy of the previously obtained customer identification data.

3. Branches/Terminals need to obtain sufficient information *to their satisfaction*, to establish the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of relationship. Being satisfied means that the *branch must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.*

4. Besides risk perception, the nature of information/documents required would also depend on the type of customer. For customers that are natural persons, branches/terminals should obtain sufficient identification data to verify the identity of the customer, his/her address, location and also his/her recent photograph.

5. For customers that are legal persons or entities, requiring an extra element of caution, branches/terminals should apply intensive Customer Due Diligence and should take reasonable measures to identify the legal entity, beneficial owner(s) and verify his/her/their identity in a manner so that the branch is satisfied that it knows who the beneficial owner(s) is/are.

6. Branches/Terminals must follow the KYC/client identification procedures guidelines as specified and strengthened by SEBI/Stock Exchanges/Depositories from time to time.

7. All the clients are to be identified in the securities market with their respective Permanent Account Number (PAN) thereby ensuring sound audit trail of all the transactions, PAN has been made sole identification number for all participants transacting in the securities market, irrespective of the amount of transaction vide SEBI Circular reference MRD/DOP/Cir-05/2007 dated April 27, 2007, subject to certain exemptions granted under circular reference MRD/DOP/MF/Cir-08/208 dated April 03, 2008 and MRD/DOP/Cir-20/2008 dated June 30, 2008.

8. Prior approval of senior management should be obtained before establishing business relationships with Politically Exposed Persons (PEP). Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, the branches/terminals should obtain senior management approval for continuing the business relationship.

9. Branches/Terminals at the time of opening accounts for PEP shall take reasonable measures to verify source of funds of clients identified as PEP.

10. The client should be identified by the branches/terminals by using reliable sources including documents / information. The branch/terminal should obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

11. The information should be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the branch/terminal in compliance with the Guidelines. Each original document should be seen prior to acceptance of a copy.

12. Branches/Terminals are required to obtain sufficient information from their Clients in order to identify and verify the identity of persons who beneficially own or control the Securities account. As per SEBI guidelines, 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 and includes a person who exercises ultimate effective control over a legal person or arrangement". Towards determination of Beneficial Ownership all the Branches/Terminals are directed to follow the guidelines given below:

A. For clients other than individuals or trusts:

Where the client is a person other than an individual or trust, viz., company, Partnership or unincorporated association/body of individuals, the Branches/Terminals shall identify the beneficial owners of the clients and take reasonable measures to verify the identity of such persons, through the following information:

- a. The identity of the natural person, who, whether acting alone or together or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

Explanation: Controlling ownership interest means ownership of/entitlement to:

- i. more than 25% of shares or capital or profits of the juridical person, where the juridical person is a company;
- ii. more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or
- iii. more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

- b. In cases where there exists doubt under clause (a) above, as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.

Explanation: Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner.

- c. Where no natural person is identified under clauses (a) and (b) above, the identity of the relevant natural person who holds the position of senior managing official.

#### B. For Client which is a Trust:

In case the client is a trust, identification of beneficial ownership to be done through the identity of the settler of the trust, the trustee, the protector, 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.

#### C. Exemption in case of listed companies:

Where the client or the owner of the controlling interest is a company listed on a Stock Exchange, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

#### D. For Foreign Investors:

Branches/Terminals dealing with foreign investors Viz., Foreign Institution Investors, Sub Accounts and Qualified Foreign Investors, may be guided by the clarifications

issued vide SEBI circular CIR/MIRSD/11/2012 dated September 5, 2012, for the purpose of identification of beneficial ownership of the client.

13. It may be noted that while risk based approach may be adopted at the time of establishing business relationship with a client, no exemption from obtaining the minimum information/documents from clients as provided in the PMLA Rules is available to brokers in respect of any class of investors with regard to the verification of the records of the identity of clients.

### Account Opening for clients

In respect of Account opening for Broking and DP for individuals under low risk category, branches/terminals shall be required to verify the following documents which may be accepted for identification and location:

- 1) PAN Card (Xerox Copy) Compulsory (**Self attested by the Client**)
- 2) Any one of the following documents for ID Proof and Address Proof (**Self attested by the Client**):

ID Proof	Address Proof
1. Passport where the address differs	1. Passport
2. Voter's Identity Card	2. Voter ID
3. Photo Identity Card issued by Govt/PSU	3. Driving License
4. Aadhaar Card	4. Bank Account Statement/Passbook Not more than 3 months old
5. Driving License	5. Ration Card
	6. Aadhaar Card
	7. Insurance Premium Receipt
	8. Flat Maintenance Bill
	9. Regd Lease or Sale agreement of Residence
	10. Utility Bills like Telephone Bill, Gas Bill, Electricity Bill not more than 3 Months old.

**Note:** Original should be produced for verification and copy, duly attested by the verifying official, should be kept along with the account opening form.

The documents listed above are only illustrative based on the list provided by regulatory authorities. Addition/Deletion/Modification to the list by the regulators, depending on subsequent developments may be accepted for identification and location from time to time.

When the aforesaid documents are accepted as the basis for opening the Stock broking and Demat **account** in the name of the holder of such document(s), the officer authorising the opening of such account must

- i. verify that the documents are prima facie in order.
- ii. ensure that the passports, identification cards, etc., are valid and are not out of date.
- iii. ensure that the signatures of the applicant and other particulars as given on the application form agrees with the signature and other particulars recorded in the above cited documents and appearance of the applicant also agrees with the photograph on the passport and/or other documents to his/her satisfaction.
- iv. note all the relevant particulars such as reference number, authority, date and place of issue, etc. of passport, voter's identity card, driving license etc., in the account opening form in the introduction columns.
- v. authenticated copies of the documents shall be obtained and keep along with the account opening form.
- vi In person verification shall be carried out certifying the documents with reference to the originals
- vii Required number of Photographs of the customers should be obtained and maintained. In case of closure of accounts the photographs should not be returned to the clients.

### **Medium / High Risk Customers**

In respect of medium/high risk customers, branches/terminals shall call for **additional** information and documentary evidence, (besides the normal documents prescribed above) which may include

<b>Type of Customers/accounts</b>	<b>Additional Information/Documents</b>
i. For opening Non Resident accounts	Passport

ii. For opening accounts of other than NRIs under Medium and High Risk categories iii. For current accounts in all risk categories iv. For accounts of other than individuals in all risk categories	In addition to obtention of documents/information for identity and location of the customer, introduction may be obtained
--	---

For customers that are legal persons or entities (i.e., other than individuals), branches should:

- a) verify the legal status of the legal person/entity through proper and relevant documents
- b) verify that any person(s) purporting to act on behalf of the legal person/entity is duly authorized and such person(s) is/are properly identified by calling for documents (as listed above for individual low risk customers) and verify the identity of that person(s)
- c) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person

If business or residential address of the prospective account holder is outside the area of operation of the branch/terminal or if the introducer is an account holder of another branch/terminal proper enquiries should be made about the reason for opening of the account. The Branch/Terminal Head has to make more enquiries than usual to test the credentials of the prospective customer before allowing him/her to open the account.

#### **Despatch of Account Opening intimation to new customers**

Service Branch will send the Account Opening Intimation to all Stock broking / Demat account customers in a closed cover.

In cases where Account Opening Intimation letters are returned undelivered for the reasons "*No such address, No such person/addressee*" and alike,

- i. 'Caution' should be noted in the Account and intimation to be given to the concerned branch/terminal.

- ii. Branch/Terminal Head/any other officer of the branch/terminal should call at the address given in the account opening form to verify whether the reason for non-delivery is correct.

**When it is established beyond doubt that the account was opened in fictitious name and Address a report should be sent to the Principal Officer immediately**

### **Monitoring of Transactions**

Regular monitoring of transactions is vital for ensuring effectiveness of the Anti Money Laundering procedures. This is possible only if the branch has an understanding of the normal activity of the client so that they can identify the deviant transactions / activities.

Branches/Terminals should pay special attention to all complex, unusually large transactions/patterns which appear to have no economic purpose. High risk accounts have to be subjected to intensified monitoring. The customer profile should be updated on a periodical basis. Wherever regulations stipulate a specific periodicity the same should be adhered to.

The Branches/Terminals and Service Branch 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 Principal Officer at Registered Office.

### **Monitoring of Suspicious Transaction & High Value Transactions**

**No cash transactions are allowed under broking. The payments to and from clients for broking operations shall be carried only through bank account. All the suspicious transactions and High Value Transactions classified below are to be identified and reported by Branches / Terminals / Service branch to the Principal Officer.**

#### **Suspicious Transaction:**

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) 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) Unusual transactions by Medium & High Risk Clients and businesses undertaken by shell corporations, offshore banks /financial services, businesses reported to be in the nature of export-import of small items.

### **High Value Transaction:**

A list of transactions which may be classified as high value transactions is given below.

- a) Under DP single transaction involving more than 25000 shares by quantity and / or Rs.5 lakhs in value.
- b) Under Stock broking single transaction of value of Rs.10.00 lakhs and above.
- c) Transaction in penny scrips (illiquid stocks notified by exchanges from time to time) when the total value of the transaction is above Rs.5.00 lakhs and or the number of shares transacted is above 1000.

Any suspicion / high value transaction should be immediately notified to the Principal Officer with details of the clients, transactions and the nature / reason of suspicion, by the branches/terminals/service branch. 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.

It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. It is clarified that branches/terminals should report all such attempted transactions to Principal Officer, even if not completed by customers, irrespective of the amount of the transaction.

### **Internal Control Systems:**

Necessary provisions would be made in the respective software for identifying and generating reports of High Value Transactions for monitoring under the guidelines.

### **Reporting to Financial Intelligence Unit - India**

In terms of the PMLA rules, the Principal Officer of the company is required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

**Director, FIU-IND, Financial Intelligence Unit-India, 6<sup>th</sup> Floor, Hotel Samrat, Chanakyapuri, New Delhi-110021. Website: <http://fiuindia.gov.in>**

The types of reports that are to be submitted are as follows:

- (a) The cash transaction report (CTR) (wherever applicable) for each month should be submitted to FIU-IND by 15<sup>th</sup> of the succeeding month.
- (b) The Suspicious Transaction Report (STR) should be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of

suspicious nature. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion.

- (c) The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND;
- (d) Utmost confidentiality should be maintained in filing of CTR and STR to FIU-IND. The reports may be transmitted by speed/registered post/fax at the notified address.
- (e) No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported.

It is also clarified that no restrictions should be put in place, on operations in the accounts where an STR has been made. It should be ensured that there is no tipping off to the client at any level when STR is made in an account.

**Modification and Review:**

The Policy guidelines shall be reviewed by the President, once a year and modified if necessary to suit the needs of the company and to comply with the regulatory requirements from time to time.