K.M.JAIN STOCK BROKERS PVT LTD-STOCK BROKER

CLIENT ACCEPTANCE POLICY
AND
RELATED WRITE-UPS
FOR NSE, BSE, MCX-SX & CDSL

POLICIES & PROCEDURES ADOPTED IN TANDEM WITH PREVENTION OF MONEY LAUNDERING ACT

Policy created by : Anand Jain

Policy reviewed by : Madhulika Jain

Policy reviewed on : 01st January, 2025

Policy approved by : Board of Directors

Policy approved on : 01st January, 2025

Table of Contents

1. Introduction

K.M.Jain Stock Brokers Pvt Ltd. (hereinafter referred to as "KMJPL", "Company", "us", "we" and "our"), is a registered Broker under SEBI Reg # INZ0003637 and Depository participant under CDSL.

2. Scope of policy

KMJPL- Customer Acceptance Policy is meant to outline the criteria for accepting new Clients and stipulates the Client categorization criteria which shall be adhered to by the Company and especially by the employees who are involved in the Client Account Opening process.

Know Your Customer Standards: Our KYC policy incorporates the following four elements:

Customer Acceptance Policy (CAP)
Customer Identification Procedures (CIP)
Monitoring of Transactions; and
Risk Management

.

3. General Principles of the Client Acceptance Policy

3.1. The General Principles of the Client Acceptance Policy are formed keeping in mind the following points before accepting the KYC form of a probable client are as follows:

3.1.1. The Company shall not conduct transactions in anonymous or fictitious names.

3.1.2. The Company shall classify Clients into various risk categories and based on the risk perception decide on the acceptance criteria for each category of Client;

3.1.3. Where the Client is a new Client, an account can be activated only after the relevant due diligence and identification measures and procedures have been conducted, according to the principles and procedures set forth in the AML (Anti Money Laundering) Guideline;

3.1.4. All documents and data required to be obtained pursuant to the Company's Client Acceptance Policy must be collected before accepting a new client

3.1.5. No Client shall be accepted in anonymous or fictitious names.

4. Criteria for accepting new clients (Based on risk)

4.1. This Section describes the criteria for accepting new Clients based on their risk categorization.

Low Risk Clients	Normal Risk Clients	High Risk Clients
The Company shall accept Clients who are categorized as low risk Clients if the general principles set forth in this CAP are implemented.	The Company shall accept Clients who are categorized as normal risk Clients if the general principles set forth hereinafter are implemented.	The Company shall accept Clients who are categorized as high-risk Clients if the general principles set forth hereinafter are implemented. Moreover, the Company shall apply the Enhanced Client Identification and Due Diligence measures for high risk Clients as applicable.

5. Low Risk Clients

5.1. The following types of Clients can be classified as low risk Clients with respect to the money laundering and terrorist financing risks, which the Company may face:

5.1.1. Non-PEP clients

5.1.2. Clients other than Hi-net worth clients

5.1.3. Entities whose identities and sources of wealth can be easily identified

5.1.4. Entities whose accounts by and large conform to the known profile

5.1.5. Clients not on any sanctions lists

5.1.6. Clients who are resident in India

The illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, only the basic requirements of verifying the identity and location of the customer shall be met.

6. Medium Risk Clients

6.1 The following types of Clients can be classified as normal risk Clients with respect to the money laundering and terrorist financing risks, which the Company may face. Customers that are likely to pose a higher than average risk to the broker may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc; such as:

6.1.1. Any client who does not fall under the "low risk Clients" or "High risk Clients" categories set forth herein.

6.1.2. Persons in business/industry or trading activity where the area of his residence or place of business has a scope or history of unlawful trading/business activity

6.1.3. Where the client profile of the person/s opening the account, according to the perception of the branch is uncertain and/or doubtful/dubious

7. High Risk Clients

7.1 The dealers may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. The following types of Clients can be classified as high-risk Clients with respect to the money laundering and terrorist financing risks, which the Company may face:

7.1.1. Non Resident Clients

7.1.2. High Net worth Individuals

7.1.3. Trusts, charities, NGOs and organizations receiving donation

7.1.4. Companies having close family shareholding or beneficial ownership

7.1.5. Firms with 'sleeping partners'

7.1.6. Politically Exposed Persons (PEPs) of foreign origin

7.1.7. Non-face to face customers

7.1.8. Those with dubious reputation as per public information available etc

7.1.9. Any other Client determined by the Company itself to be classified as such.

8. Unacceptable Clients

8.1. The following list predetermines the types of Clients who are not acceptable for establishing a Business Relationship with the Company.

8.1.1. Clients who fail or refuse to submit, the requisite data and information for the verification of their identity and the creation of their economic profile, without adequate justification;

8.1.2. The Company shall not conduct transactions in cases where the identity of the client matches with any person with known criminal background or with banned entities such as individual terrorists or terrorist organization's etc. whose name appear in the lists/s published from time to time

8.1.3. Any other Clients that their nature of business entail a higher risk of money laundering or terrorist financing

8.1.4. Any other Clients that their nature entail a higher risk of money laundering or terrorist financing

8.1.5. Clients from countries that is considered inadequately the FATF and its rules & regulations

8.1.6. Any other Client determined by the Company itself to be classified as such

9. Transactions by Politically Exposed Persons (PEPs)

9.1. PEPs or Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in India or a foreign country e.g. Heads of States or of Governments, Senior Politicians/Government/Judicial, important political officials etc.

9.2. Before accepting PEP as a customer, the Company will identify him/her and confirm the sources of funds.

9.3. The decision to continue business relations with PEPs would be taken at Board level.

10. CSC- Clients of Special category

10.1 Such clients include the following

10.1.1. Non resident clients

10.1.2. High net worth clients

10.1.3. Trust, Charities, NGOs and organizations receiving donations

10.1.4. Companies having close family shareholdings or beneficial ownership

10.1.5. Politically exposed persons (PEP) of foreign origin

10.1.6. 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)

10.1.7 Companies offering foreign exchange offerings

10.1.8 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.

10.1.9. Non face-to-face clients

10.1.10 Clients with dubious reputation as per public information available etc.

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

The dealers shall collect documents and other information from the customer depending on perceived risk and keeping in mind the requirements of AML Act, 2002 and guidelines issued by RBI from time to time.
The dealers shall close an existing account or shall not open a new account where it is unable to apply appropriate customer due diligence measures i.e., branch is unable to verify the identity and/or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of data/information furnished to the branch.
The dealers shall, however, ensure that these measures do not lead to the harassment of the customer. However, in case the account is required to be closed on this ground, the dealers shall do so only after permission of Senior Official of their concerned Offices is obtained. Further, the customer should be given a prior notice of at least 20 days wherein reasons for closure of his account should also be mentioned.
The dealers shall make necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc. RBI has been circulating lists of terrorist entities notified by the Government of India so that brokers exercise caution against any transaction detected with such entities. The dealers shall invariably consult such lists to ensure that prospective person/s or organizations desirous to establish relationship with the broker are not in any way involved in any unlawful activity and that they do not appear in such lists.
The dealers shall prepare a profile for each new customer based on risk categorization. The broker has devised a revised Composite Account Opening Form for recording and maintaining the profile of each new customer. Revised form is separate for Individuals, Partnership Firms, Corporate and other legal entities, etc. The nature and extent of due diligence shall depend on the risk perceived by the dealer. The dealers should continue to follow strictly the instructions issued by the broker regarding secrecy of customer information. The dealers should bear in mind that the adoption of customer acceptance policy and its implementation does not become too restrictive and should not result in denial of brokering services to general public, especially to those, who are financially or socially disadvantaged.

11. Client Application due diligence and identification procedures

11.1. The Company shall duly apply Client identification procedures and Client due diligence measures in the following instances:

11.1.1. When establishing a Business Relationship;

11.1.2. When there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction;

11.1.3. When there are doubts about the veracity or adequacy of previously Client identification data.

12. Customer Identification Procedure (CIP)

12.1. The Company's customers need to be verified in line with Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Sufficient information needs to be obtained to the satisfaction, which is necessary to establish, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of relationship.

12.2. While opening the account of the customer or during periodic updating, the Company shall seek 'mandatory' information required for KYC purpose, which the customer is obliged to give.

12.3. The following table will be referred for customer identification and verification procedure:

Client's-Constitution	**Proof of identity**	**Proof of Address**	**Others**
Individual	1. Pan card	1. Copy of bank Statement etc.	1. N.A
Company	1.Pan card 2.Certificate of Incorporation 3. Memorandum & Articles 4. Board Resolution	1.. As Above	1. Proof of Identity of Directors/others authorized to trade
Partnership Firm	1. Pan Card 2. Registration certificate 3. partnership deed	1. As above	1. Proof of Identity of partners/others authorized to trade
Trust	1. Pan Card 2. Registration certificate 3. Trust deed	1 As above	1. Proof of Identity of trustees/others authorized to trade
AOP/BOI	1 Pan Card 2. Resolution of Management 3. Certificate of legal Existence	1 As above	1 Proof of Identity of persons/others authorized to trade

Notes:
All Pan cards to be verified from Income Tax/ NSDL sites before the account is opened
If a potential customer refuses to provide the above details or willfully provides misleading details, then our firm will not open the trading account.
Client records will be maintained for 10 years after closure of Trading account of any client
Reluctance on the part of the client to provide necessary information or cooperate in verification process could generate a red flag for the member for additional monitoring.

13. Monitoring & Reporting of Suspicious Transactions:

13.1 Ongoing monitoring of accounts is an essential element of an effective Anti Money Laundering framework. Such monitoring should result in identification and detection of apparently abnormal transactions, based on laid down parameters. Members should devise and generate necessary reports/alerts based on their client's profile, nature of business, trading pattern of clients for identifying and detecting such transactions. These reports/alerts should be analyzed to establish suspicion or otherwise for the purpose of reporting such transactions .Ongoing monitoring is an essential element of effective KYC procedures. Risk can be effectively controlled and reduced after understanding the normal and reasonable activity of the customer vis-a-vis transactions that fall outside the regular pattern of activity. However, the extent of monitoring shall depend on the risk sensitivity of the account.

Ongoing due diligence with respect to the business relationship with every client shall be exercised and the transactions shall be examined closely to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds Ongoing monitoring is an essential element of effective KYC procedures. Risk can be effectively controlled and reduced after understanding the normal and reasonable activity of the customer vis-a-vis transactions that fall outside the regular pattern of activity. However, the extent of monitoring shall depend on the risk sensitivity of the account. Ongoing due diligence with respect to the business relationship with every client shall be exercised and the transactions shall be examined closely to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds.

13.1.1 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:

i) Clients whose identity verification seems difficult or clients appear not to cooperate
ii) Substantial increase in activity without any apparent cause
iii) Large number of accounts having common parameters such as common partners / directors / promoters / address / email Address / telephone numbers / introducers or authorized signatories;
iv) Transactions with no apparent economic or business rationale
v) Sudden activity in dormant accounts;
vi) Source of funds are doubtful or inconsistency in payment pattern;
vii) Unusual and large cash deposits made by an individual or business;
viii) Transfer of investment proceeds to apparently unrelated third parties;
ix) Multiple transactions of value just below the threshold limit specified in PMLA so as to avoid possible reporting;
x) Unusual transactions by CSCs and businesses undertaken by shell corporations, offshore banks /financial services businesses reported to be in the nature of export-import of small items.;
xi) Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;
xii) Clients in high-risk jurisdictions or clients introduced by banks or affiliates or other clients based in high risk jurisdictions;
Xiii) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
xiv) Purchases made on own account transferred to a third party through off market transactions through DP Accounts;
xv) Suspicious off market transactions;
xvi)Large deals at prices away from the market.
xvii) Accounts used as 'pass through'. Where no transfer of ownership of securities or trading is occurring in the account and the account is being used only for funds transfers/layering purposes.
xviii)Trading activity in accounts of high risk clients based on their profile, business pattern and industry segment.

13.1.2 Broad categories for reason of suspicion are given below:

- Suspicious criminal background of the client
- Multiple accounts having common account holder or introducer or authorized signatory with no rationale
- Unusual activity in dormant accounts or in aberration to past activities
- Source of funds are doubtful
- Appears to be case of insider trading
- Suspicious off-market transactions
- Value of transaction being inconsistent to client's financial standing

14. Reporting of Suspicious Transactions to FIU IND

14.1 The Company undertakes to report any Suspicious Activities in line with the requirements of the Financial Intelligence Centre (FIC).Information to be reported concerning property associated with terrorist and related activities. Processes for alert generation, examination and reporting should include:

14.1.1 Audit trail for all alerts generated till they are reported to FIU / closed
14.1.2 Clear enunciation of responsibilities at each stage of process from generation, examination, recording and reporting
14.1.3 Escalation through the organization to the principal officer designated for PMLA
14.1.4 Confidentiality of STRs filed

14.1.5 Retention of records

14.1.6 Reporting of Suspicious Transactions

14.1.7 Cash threshold reporting

14.1.8 All cash transaction requiring reporting will be done in CTR format and in the manner and at intervals prescribed by FIU IND. We will make a note of all transactions that have not been explained to the satisfaction of our principal officer and thereafter report the same to FIU IND. Wherever we have reason to suspect any criminal activity, illegal activity, activity involving evasion of PMLA regulations and unlawful business activity, then the same would be tracked and reported promptly. As and when any suspicious transactions or any transaction whether within the permissible regulation limits but constituting an anomaly would be tracked and reported to FIU/BSE/SEBI/CDSL or concerned regulatory bodies. For CDSL-"*Blng024900_fui"* file should be monitored for abnormal DP transactions on fortnightly basis or as and when received from CDSL. Any aberrations should be noted. Possibility of fraudulent or suspicious trades should be traced, inquired for and then reported to the concerned authority.

14.1.9 In terms of the PML Rules, intermediaries are 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,
6th Floor, Hotel Samrat,
Chanakyapuri, New Delhi-110021.
Website: http://fiuindia.gov.in

Intermediaries shall carefully go through all the reporting requirements and formats enclosed with this circular. These requirements and formats are divided into two parts- Manual Formats and Electronic Formats. Details of these formats are given in the documents (Cash Transaction Report- version 1.0 and Suspicious Transactions Report version 1.0) which are also enclosed with this circular. These documents contain detailed directives on the compilation and manner/procedure of submission of the manual/electronic reports to FIU-IND. The related hardware and technical requirement for preparing reports in manual/electronic format, the related data files and data structures thereof are also detailed in these documents. Intermediaries, which are not in a position to immediately file electronic reports, may file manual reports with FIU-IND as per the formats prescribed. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, intermediaries shall adhere to the following:

The Cash Transaction Report (CTR) (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month. The Suspicious Transaction Report (STR) shall 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 shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion. The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND; Utmost confidentiality shall 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. No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported.

Intermediaries shall not put any restrictions on operations in the accounts where an STR has been made. Intermediaries and their directors, officers and employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU-IND. This prohibition on tipping off extends not only to the filing of the STR and/or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the client at any level. It is clarified that the registered intermediaries, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

15. AML Record keeping

15.1.1. *STR Maintenance and confidentiality*

Confidentiality of STRs and other supporting documents will be maintained. Only law enforcement or regulatory authorities need be informed about it. Any request for STR information would not be entertained and request will be informed to FIU IND immediately. Separate filing for STRs will be maintained. Principal Officer will handle all requests related to it.

15.1.2. *Responsibility for AML records and SAR filing*

Principal Officer will be in charge of record keeping of STRs.

15.1.3. *Records required*

As part of our AML program, our firm will create and maintain STRs and CTRs and other relevant documentation about customer identity/verification. Such records will be maintained for at least ten years.

16. Record maintenance: Record keeping/ Retention of records/Freezing of Records

16.1 The principal officer should maintain such records that 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.

16.1.1 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.

16.1.2 Registered Intermediaries should ensure that all customer and transaction records and information are available on a timely basis to the competent investigating authorities. Where appropriate, they should consider retaining certain records, e.g. customer identification, account files, and business correspondence, for periods which may exceed that required under the SEBI Act, Rules and Regulations framed there-under PMLA 2002, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.

16.1.3 More specifically, all the intermediaries shall put in place a system of maintaining proper record of transactions prescribed under Rule 3, notified under the Prevention of Money Laundering Act (PMLA), 2002 as mentioned below:
(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 exceeds 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.

16.1.4 Intermediaries are required to maintain and preserve the following information in respect of transactions 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.

16.1.5 *Retention of Records*
Intermediaries should take appropriate steps to evolve an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities. Further, the records mentioned in Rule 3 of PMLA Rules have to be maintained and preserved for a period of ten years from the date of cessation of the transactions between the client and intermediary.

16.1.6 As stated in para 5.5, intermediaries are required to formulate and implement the client identification program containing the requirements as laid down in Rule 9 and such other additional requirements that it considers appropriate. The records of the identity of clients have to be maintained and preserved for a period of ten years from the date of cessation of the transactions between the client and intermediary.

16.1.7 Thus 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), account files and business correspondence should also be kept for the same period.

16.1.8 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.

17 Ongoing training to Employees:

17.1 Principal Officer would be responsible to impart necessary training to employees. Employees will be sensitized of the requirements under PMLA and the procedures laid down by the member.

17.1.1 It will be ensured that all the operating and management staff fully understands their responsibilities under PMLA for strict adherence to customer due diligence requirements from establishment of new accounts to transaction monitoring and reporting suspicious transactions to the FIU.

17.1.2 Annually, training programmes would be imparted wherever required for new staff, front-line staff, sub-brokers, supervisory staff, controllers and product planning personnel, etc.

17.1.3 Training may include written materials like pamphlets, audio/video Cds, in-person lectures and professional seminars. Employees of the compliance department should be asked to attend BSE/NSE/CDSL Compliance training program.

18 Reliance on third party for carrying out Client Due Diligence (CDD)

18.1 Registered intermediaries 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. 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. Regular review of CDD to be undertaken annually or as and when any important notification/s is/are issued by the authorities.

19. e-KYC Authentication facility under section 11A of the Prevention of Money Laundering Act, 2002 by Entities in the securities market for Resident Investors

19.1 Circular # SEBI/HO/MIRSD/DOP/CIR/P/2019/123 November 05, 2019

19.1.1 Entities in the securities market, as may be notified by the Central Government, shall be allowed to undertake Aadhaar Authentication under section 11A of the PMLA. SEBI Registered intermediaries for reasons such as online on-boarding of clients, customer convenience, increased efficiency and reduced time for client on-boarding would prefer to use Aadhaar based e-KYC facility to complete the KYC of the client.

19.1.2 These entities would be registered with UIDAI as KYC user agency ("KUA") and shall allow all the SEBI registered intermediaries / mutual fund distributors to undertake Aadhaar Authentication of their clients for the purpose of KYC through them. For detailed procedure SEBI Circular # SEBI/HO/MIRSD/DOP/CIR/P/2019/123 November 05, 2019, should be referred.

20. Policy to share KYC Information as permitted by Law

SEBI CIR/ IMD/ FIIC/ 11/ 2014- June 16, 2014

Process to be followed by DDPs to share the relevant KYC documents of FPIs with the banks and record of transfer of documents

20.1.1 In the light of the above circular, it has been decided as follows:

a. DDPs are advised to share the relevant KYC documents with the banks concerned based on written authorization from the FPIs.

b. Accordingly, a set of hard copies of the relevant KYC documents furnished by the FPIs to DDPs may be transferred to the concerned bank through their authorised representative.

c. While transferring such documents, DDPs shall certify that the documents have been duly verified with the original or notarized documents have been obtained, where applicable. In this regard, a proper record of transfer of documents, both at the level of the DDP as well as at the bank, under signatures of the officials of the transferor and transferee entities, may be kept.