MONEDO FINANCIAL SERVICES PVT. LTD.

KYC AND AML POLICY

Contents

18. Risk Management

19. Updation / Periodic Updation of KYC

20. Compliance of KYC Policy

21. Policy Implementation Guidelines

    - Customer Education
    - Introduction of new technologies
    - Applicability to branches and subsidiaries outside India
    - KYC Policy for existing customers

22. Appointment of Principal Officer and Role of Principal Officer

23. Money Laundering and Terrorist Financing Risk Assessment and Monitoring of Risk- Adopting Risk based Approach

24. Combating financing of terrorism

25. Countries which do not or insufficiently apply the FATF recommendations

26. Inter-Governmental Agreement (IGA) with United States of America (US) under Foreign Accounts Tax Compliance Act (FATCA) – Registration

27. Constitution of Special Investigating Team – sharing of information

1. INTRODUCTION:

The objective of KYC/AML/CFT guidelines is to prevent banks, NBFCs from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. In order to prevent banks and other financial institutions from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of prescribing various rules and regulations. Internationally, the Financial Action Task Force (FATF) sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. India, being a member of FATF, is committed to upholding measures to protect the integrity of international financial system.

In India, the **Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005**, form the legal framework on Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT). In terms of the provisions of the PML Act, 2002 and the PML Rules, 2005, as amended from time to time by the Government of India, Regulated Entities (REs) are required to follow the instructions contained therein in letter and spirit for combating money laundering, terrorist financing and other related threats to the integrity of the financial system

2. SCOPE AND APPLICATION OF THE POLICY

The scope of this policy is:

- To lay down explicit criteria for acceptance of customers.
- To establish procedures to identify of individuals/non-individuals for opening of account.
- To establish processes and procedures to monitor high value transactions and/or transactions of suspicious nature in accounts.
- To develop measures for conducting due diligence in respect of customers and reporting of such transactions.

To fulfil the scope, the following four key elements will be incorporated into our policy:

- Customer Acceptance Policy
- Customer Identification Procedures
- Monitoring of Transactions
- Risk Management

3. CUSTOMER ACCEPTANCE POLICY

The entity has a Customer Acceptance Policy to ensure that no account is opened or transaction or account based relationship is established containing defined norms and procedures in relation to its' customers. In line with the policy, the entity shall implement a CDD (Customer Due Diligence) programme, having regard to the ML/TF risks identified and the size of business. Further, Monedo Financial Services Private Limited "Entity" is monitoring the implementation of the controls and enhance them if necessary. The Company has Customer Due Diligence (CDD) Procedure for identification and acceptance of prospective customers.

However, Customer Acceptance Policy framed, shall not result in denial of banking /financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

Definition of a Customer

- A person or entity that maintains an account and/or has a business relationship with the Company
- One on whose behalf the account is maintained (i.e. the beneficial owner)
- Beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers
- Chartered Accountants, Solicitors etc. as permitted under the law, and
- Any other person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company, say a wire transfer or issue of high value demand draft as a single transaction.

A "Person" shall have the meaning as defined under KYC policy of RBI (and any amendment from time to time by RBI) which at present is as follows:

'Person' shall include:

a. an Individual;
b. a Hindu Undivided Family;
c. a Company;
d. a Firm;
e. an association of persons or a body of individuals, whether incorporated or not;
f. every artificial juridical person, not falling within any one of the above person (a to e);
g. any agency, office or branch owned or controlled by any one of the above persons (a to f)

4. GUIDELINES FOR ACCEPTING CUSTOMERS- DUE DILIGENCE OF CUSTOMERS – RELIANCE ON THIRD PARTY FOR DUE DILIGENCE OF CUSTOMERS

Under the Customer Acceptance Policy, the norms and procedures which the entity would observe and ensure for accepting the customers for entering into account opening and transaction-based relationship, are as under:

(a) No loan account account is opened in anonymous or fictitious/benami name.

(b) No loan account is opened where the entity is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The RE shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.

(c) No transaction or account-based relationship is undertaken without following the CDD procedure.

(d) The mandatory information to be sought for KYC purpose while opening a loan account and during the periodic updation, is specified.

(e) Additional information, where such information requirement has not been specified in the internal KYC Policy of the entity, is obtained with the explicit consent of the customer.

(f) The entity shall apply the CDD procedure at the UCIC (Unique Customer Identification Code) level.

(g) CDD Procedure is followed for all the joint account holders, while opening a joint account.

(h) Circumstances in which a customer is permitted to act on behalf of another person/entity are clearly spelled out.

(i) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists as notified from time to time either by Govt. of India, State Govt. Or any other National/International body/organization or as indicated in Chapter IX of RBI Master Direction – Know Your Customer (KYC) Direction, 2016 as updated.

(j) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

(k) Where an equivalent e-document is obtained from the customer, The entity verify the digital signature as per the provisions of the Information Technology Act, 2000.

(l) Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

Due Diligence of Customers- Reliance on Third party for customer due diligence

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the entity may rely on a third party subject to the following conditions that-

- the entity immediately obtains necessary information of such client due diligence carried out by the third party;
- the entity takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
- the entity is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act;
- the third party is not based in a country or jurisdiction assessed as high risk and
- the entity is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable

Further, the entity should undertake **on-going due diligence of customers** to ensure that their transactions are consistent with their knowledge about the customers, customers'. business and risk profile, the source of funds / wealth. For ongoing due diligence, It may also consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

The entity adopt a **risk-based approach for periodic updation of KYC** ensuring that the information or data collected under **CDD** is kept up-to-date and relevant, particularly where there is high risk.

Customer Due Diligence (CDD) Procedure in case of Individuals:

For undertaking CDD, REs shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

(a) the Aadhaar number where,

(i) he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or

(ii) he decides to submit his Aadhaar number voluntarily to a bank or any entity notified under first proviso to sub-section (1) of section 11A of the PML Act; or

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

(ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; or

(ac) the KYC Identifier with an explicit consent to download records from CKYCR; and

(b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

(c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the entity.

Provided that where the customer has submitted,

i) Aadhaar number under clause (a) above to a entity notified under first proviso to sub-section (1) of section 11A of the PML Act, such entity shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the entity.

ii) proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the entity shall carry out offline verification.

iii) an equivalent e-document of any OVD, the entity shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo.

iv) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the RE shall carry out verification through digital KYC.

v) KYC Identifier under clause (ac) above, the entity shall retrieve the KYC records online from the CKYCR in accordance with Section 56.

Provided that for a period not beyond such date as may be notified by the Government for a class of entity, instead of carrying out digital KYC, the entity pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016

owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, Entity shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the entity and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. Entity shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the entity and shall be available for supervisory review.

Accounts opened using Aadhaar OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:

i. There must be a specific consent from the customer for authentication through OTP.

ii. As a risk-mitigating measure for such accounts, entity ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. Entity have a board approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts.

iii. The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (vi) below is complete.

iv. The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.

v. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.

vi. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 16 or as per Section 18 (V-CIP) is carried out. If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

vii. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.

viii. A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in nonface- to-face mode with any other emtity. Further, while uploading KYC information to CKYCR, entity shall clearly indicate that such accounts are opened using OTP based e-KYC and other entity shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-faceto- face mode.

Entity shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

Enhanced Due Diligence for non-face- to -face customers onboarding may be followed. Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP (Video based Customer Identification process).

5. OFFICIALLY VALID DOCUMENT

"Officially Valid Document" (OVD) means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

6. RISK LEVEL CATEGORIZATION

Risk Categorization forms an essential part of the risk management. The entity should lay down broad principles for risk categorization of customers.

- Risk categorization shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

- The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer

i. **Type of low risk customers**- individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorized as low risk. Illustrative examples of low risk customers may include government departments and government owned companies, regulators and statutory bodies, etc.

   In such cases, the policy requires only the basic requirements of verifying the identity an location of the customer.

ii. **Type of medium or high-risk customers** - Customers that are likely to pose a higher than average risk to DMI may be categorized as medium or high risk depending on the customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc. DMI will 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. Examples of customers requiring higher due diligence may include

   (i) Trusts, charities, NGOs and organizations receiving donations,

   (ii) Companies having close family shareholding or beneficial ownership,

   (iii) Firms with 'sleeping partners',

   (iv) Politically exposed persons (PEPs) of foreign origin,

   (v) Non-face to face customers, and

   (vi)Those with dubious reputation as per public information available, etc. DMI has

formulated an indicative list of customers and their respective risk categories. Please find attached as Annexure-A.

7. DUE DILIGENCE OF BUSINESS PARTNERS

The following due diligence must also be performed on prospective Business Partners.

A) Verify Identity:

i. Obtain and file legible copies of corporate formation and registration documents or publiccompany prospectuses and government filings.
ii. PAN card of the Directors etc.
iii. Wherever possible (in the case of privately owned entities), arrange for recommendation from legal counsel to the company.
iv. Wherever possible (in the case of privately owned entities), obtain from appropriate government entity confirmation of due incorporation and existence of the corporation.

B) Verify Source of Income:

i. Research for the Company details in available news or business databases and obtain allcorporate earnings information available.

The Company shall maintain files on each Business Partner with copies of all data obtained and memorialize in writing all the verification efforts. These files may be maintained electronically and should be accessible quickly when needed.

8. DUE DILIGENCE ON EMPLOYEES

The Company shall perform the following Due Diligence on Prospective Employees prior to their date of joining

A) Verify Identity:

i. Obtain originals of and file legible copies of identification documents that contain photographs of theindividual. Acceptable examples include:

- Passports (obtain all nationalities an individual may have)
- PAN card
- Driver's license
- UID or Physical Aadhaar card/letter or e-Aadhaar letter
- Voter's Identity Card

B) Verify Domicile of Residence:

i. Example: Obtain copies of utility bill receipts or other form of objective verification of Residence, UID or Physical Aadhaar card/letter or e-Aadhaar letter (if the address provided by the customer is the same on the document submitted for identity proof)

C) Verify the previous year's Employment Record:

i. Obtain and call the previous employer to check the credentials of the prospective employee

ii. Check and verify the address of employee

D) Check References:

i. Obtain 2 or more professional employment references from the prospective employee.

ii. The prospective manager of the employee, or, the Human Resources department, must personally converse with the prospect's references The Company shall maintain files for each employee hired together with copies of all data obtained. These files may be maintained in electronic or physical form and should be accessible quickly when needed.

Further these files will be classified as confidential data and details contained therein shall notbe divulged for cross selling or any other purpose.

9. PURPOSEFUL IMPLEMENTATION

The purpose of adopting the above measures and norms while taking decisions on the issue of customeracceptance is twofold. Firstly, the Company should not suffer financially at later stage due to lack of proper due diligence exercise and lack of information which is the exclusive possession of the customers.

Secondly, to curb and prevent any such practice by the customers which is aimed to achieve unlawful objectives or any other practice by which the financial institutions can be used to perpetuate any criminal or unlawful activities. However, at the same time, this policy does not aim or intend to deny the benefit of financial services to those who genuinely need such services / facilities due to real lack of their own sufficient financial resources.

10. CUSTOMER IDENTIFICATION PROCEDURE (CIP)

Customer identification means identifying the customer and verifying his / her identity by using reliable,independent source documents, data or information. The Company needs to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship. Being risk perception, thenature of information / documents required would also depend on the type of the customer (individual,corporate etc.)

NEED FOR PHOTOGRAPHS

- In case of change in the authorized signatories, photograph of the new signatory should be obtained duly countersigned by the competent authorities of the concerned institution / organization;
- Where the account is operated by the letters of Authority or Power of Attorney Holder, photograph of the authority holder should be obtained duly attested by the Borrower / Depositor.

PROOF OF CUSTOMERS' ADDRESS

A detailed list of the features to be verified and documents that may be obtained from the Customers are given below. A Photostat copy of the proofs mentioned in below should be filed along with the loan application. In case of need, the Company Manager can depute an official to visit the account holder / loan applicant at the given address to satisfy about the genuineness of the address.

List of documents for address proof:

1. Aadhaar card
2. Voter ID Card
3. Driving License

4. Passport
5. Electricity Bill

The entity should undertake identification of customers in the following cases:

(a) Commencement of an account-based relationship with the customer.
(b) Carrying out any international money transfer operations for a person who is not
(c) an account holder of the entity. when there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
(d) Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.
(e) Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
(f) When a entity has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
(g) entity shall ensure that introduction is not to be sought while opening accounts.

11. DIGITAL KYC PROCESS

(a) The entity developed an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the entity.

(b) The access of the Application shall be controlled by the entity and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by entity to its authorized officials.

(c) The customer, for the purpose of KYC, shall visit the location of the authorized official of the entity or vice-versa. The original OVD shall be in possession of the customer.

(d) The entity must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the entity shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by entity) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

(e) The Application of the entity shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.

(f) Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

(g) The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

(h) Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e- Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

(i) Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the entity shall not be used for customer signature. The entity must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

(j) The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the RE. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

(k) Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the RE, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

(l) The authorized officer of the entity shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.

(m) On Successful verification, the CAF shall be digitally signed by authorized officer of the entity who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

12. PROVISIONS UNDER PMLA

As per the provisions of Rule 9 of the Prevention of Money Laundering (Maintenance of Records of theNature and Value of Transactions, The Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 (hereinafter referred to as PML Rules), the Company shall:

- At the time of commencement of an account-based relationship, identify its clients, verify their identity and obtain information on the purpose and intended nature of the business relationship and
- In all other cases, verify identify while carrying out:

  ✓ Transaction of an amount equal to or exceeding rupees fifty thousand, whether

conductedas a single transaction or several transactions that appear to be connected,

- ✓ Any international money transfer operations.

In terms of proviso to rule 9 of the PML Rules, the relaxation, in verifying the identity of the client within a reasonable time after opening the account / execution of the transaction, stands withdrawn.

Abiding by the provisions of Rule 9, the Company shall identify the beneficial owner and take all reasonable steps to verify his identity. The said Rule also require that the Company should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions to ensure that they are consistent with their knowledge of the customer, his businessand risk profile.

Customer identification requirements keeping in view the provisions of the said rule are given in "Annexure-2" for guidance of the Company.

Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Amendment Rules, 2009/10 - Obligation of banks/Financial institutions.

Government of India vide its Notifications No.13/2009/F.No.6/8/2009-ES dated November 12, 2009, February 12, 2010 and June 16, 2010 amended the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005.

- The Entity is strictly follows the amended provisions of PMLA Rules and ensure meticulous compliance with these Rules.

13. MONITORING OF TRANSACTIONS AND MAINTENANCE OF RECORDS OF TRANSACTIONS

Monitoring of Transactions:

- Ongoing monitoring is an essential element of effective KYC procedures. Hence, the entity examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations.

- Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible be examined, and written findings together with all documents be retained and made available to Reserve Bank/other relevant authorities, on request.

- The entity should apply enhanced due diligence measures on high risk customers. In view of the risks involved in cash intensive businesses, accounts of bullion dealers (including sub-dealers) and jewelers should also be categorized by NBFCs as 'high risk' requiring enhanced due diligence.

- Entity is also required to subject these 'high risk accounts' to intensified transaction monitoring. High risk associated with such accounts should be taken into account by entity to identify suspicious transactions for filing Suspicious Transaction Reports (STRs) to FIU-ND.

Maintenance of records of transactions:

The entity have a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005), as mentioned below:

(i) all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;

(ii) Series of all cash transactions individually valued below Rupees Ten Lakh, or its equivalent in foreign currency which have taken place within a month and the monthly aggregate which exceeds rupees ten lakhs or its equivalent in foreign currency. It is clarified that for determining 'integrally connected transactions' 'all accounts of the same customer' should be taken into account.

(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 facilitating the transactions;

(iv) all suspicious transactions whether or not made in cash and in manner as mentioned in the Rules framed by Government of India under the Prevention of Money Laundering Act, 2002.

The entity is adhere to the reporting requirements as per the amended rules as under:

Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following information:

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

14. PRESERVATION OF RECORDS

- The entity should take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

- In terms of PML Amendment Act 2012, the entity should maintain for at least five years from the date of transaction between the entity and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

- The entity should ensure that records pertaining to the identification of the customers and their address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills, etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended as required under Rule 10 of the Rules ibid. The identification of records and transaction data should be made available to the competent authorities upon request.

- The entity shall maintain records of the identity of their clients, and records in respect of transactions referred to in Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005) in hard or soft format.

- The entity is required to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the backgroun d including all documents/office records/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level should be properly recorded. Such records and related documents should be made available to help auditors to scrutinize the transactions and also to Reserve Bank/other relevant authorities. These records are required to be preserved for five years as is required under PMLA, 2002.

15. REPORTING TO FINANCIAL INTELLIGENCE UNIT-INDIA – CTR (CASH TRANSACTION REPORT) AND STR (SUSPICIOUS TRANSACTION REPORT) AND CCR (COUNTERFEIT CURRENCY REPORT) SUBMISSION

In terms of the PMLA rules, the entity 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, 6th Floor, Hotel Samrat, Chanakyapuri, New Delhi-110021

Website - http://fiuindia.gov.in/

There are altogether **five reporting formats** prescribed for a Financial institutions viz. i) Manual reporting of cash transactions ii) Manual reporting of suspicious transactions iii) Consolidated reporting of cash transactions by Principal Officer of the entity iv) Electronic data structure for cash transaction reporting and v) Electronic data structure for suspicious transaction reporting. The reporting formats contain detailed guidelines on the compilation and manner/procedure of submission of the reports to FIU-IND.

- The entity is adopting the format prescribed for NBFCs with suitable modifications.

- The entity initiated steps to ensure electronic filing of cash transaction report (CTR). The related hardware and technical requirement for preparing reports in an electronic format, the related data files and data structures thereof were furnished in the instructions part of the concerned formats. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, the entity should scrupulously adhere to the following:

- **The cash transaction report (CTR)** for each month should be submitted to FIU-IND by 15th of the succeeding month. While filing CTR, individual transactions below rupees fifty thousand may not be included. Cash transaction reporting by branches/offices of the entity to their Principal Officer should invariably be submitted on monthly basis (not on fortnightly basis) and the Principal Officer, in turn, should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule;

- **The Suspicious Transaction Report (STR)** should be furnished 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 once a suspicious transaction report is received from a branch or any other office. Such report should be made available to the competent authorities on request.

- A separate **Counterfeit Currency Report (CCR)** should be filed for each incident of detection of forged/counterfeit Indian Currency. If the detected counterfeit currency notes can be segregated on the basis of tendering person, A separate CCR should be filed for each such incident. These transactions should be reported to Director, FIU-IND, by not later than 15th of the succeeding month from the date of occurrence of such transactions.

All branches of the company (where applicable) have been provided with machines for detection of forged notes, in the event of any forged /counterfeit is detected by branch staff, despite taking all precautions; then it must be noted in a Cash Register separately.

Reporting of the case with full details like name, of customer, amount, denomination, date must be reported by branch manager to Compliance department at HO with copy to National Head- Branch Business and Zonal Head.

All cash transactions (where forged /counterfeit Indian Currency has been used as genuine) should also include transactions where forgery of valuable securities/documents have taken place and the same may be reported to FIU-IND in plain text format.

16. OTHER ESSENTIAL ASPECTS RELATED TO CTR AND STR REPORTING

In regard to CTR, the cut-off limit of Rupees ten lakh is applicable to integrally connected cash transactions also. Further, after consultation with FIU-IND, it is clarified that:

- For determining integrally connected cash transactions, the entity should consider all individual cash transactions in an account during a calendar month, where either debit or credit summation, computed separately, exceeds Rupees ten lakh during the month. However, while filing CTR, details of individual cash transactions below rupees fifty thousand may not be indicated.

- CTR should contain only the transactions carried out by the entity on behalf of their clients/customers excluding transactions between the internal accounts of the entity ;

- All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported by the Principal Officer to FIU-IND immediately in the format (Counterfeit Currency Report – CCR). These cash transactions should also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

- While making STRs, the entity should be guided by the definition of 'suspicious transaction' as contained in Rule 2(g) of Rules ibid. The entity should make STRs if they have reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

- The entity may take note of the **timeliness of the reporting requirements**. In terms of Rule 8, while furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall constitute a separate violation.

- The entity is required to prepare a **profile for each customer based on risk categorization** in terms of instructions contained in the guidelines on 'Know Your Customer Norms' and 'Anti-Money Laundering Measures' of RBI circular. Further, the need for periodical review of risk categorization has been emphasized. The entity, as a part of transaction monitoring mechanism, is required to put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers. It is needless to add that robust software throwing alerts is essential for effective identification and reporting of suspicious transactions.

- The entity is required to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background including all documents/office records/memorandums pertaining to such transactions and the purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level should be properly recorded. **These records are required to be preserved for ten years as is required under PMLA, 2002**. Such records and related documents should be made available to help auditors in their work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities.

17. MONITORING & REPORTING OF TRANSACTIONS

The Company will keep a continuous vigil, if any of the following acts or events is noticed in relation tothe customer's approach or behaviour while dealing with the Company:

1. Reluctance of the customer to provide confirmation regarding his identity
2. Loan money is used for the purpose other than the one mentioned in the sanction letter form and the real purpose is not disclosed to the Company
3. Customer forecloses the loan prior to the stated maturity
4. Customer suddenly pays a substantial amount towards partial repayment of the loan
5. Customer defaults regularly and then pays substantial cash at periodical intervals i.e. once in sixmonths.

The Company shall pay special attention to all complex, high-risk, unusually large transactions and all unusual or suspicious patterns which have no apparent economic or visible lawful purpose.

The Company may prescribe threshold limits for a particular category of accounts and pay close attention to the transactions that exceed the prescribed threshold limits. Keeping this in view, the Company shall pay particular attention to the cash transactions which exceed the limits of Rs. 10 lakhs,either per transaction or credit and debit summation in a single month. This would include transactionwhere the customer by way repayment of loan, whether in part or full, deposit Rs. 10 lakhs and abovein cash. Such transactions shall be reported to the Risk Department and the Principal Officer appointedas per this policy. In such cases, the Company shall keep a close and careful watch on the subsequent mode of payments adopted by such customer.

Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer shall attract special attention of the Company. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through that account. Company shall ensure that proper record of all transactions and cash transactions (deposits and withdrawals) of Rs.10 lakhs and above in the accounts is preserved and maintained as required under the PMLA.

The information in respect of the transactions referred to in clauses I, II and III referred above will be submitted to the Director - FIU every month by the 15th day of the succeeding month.

The information in respect of the transactions referred to in clause IV referred above will be furnishedpromptly to the Director - FIU in writing, or by fax or by electronic mail not later than seven working days from the date of occurrence of such transaction.

The information in respect of the transactions referred to in clause V referred above will be furnished promptly to the Director - FIU in writing, or by fax or by electronic mail not later than seven working days on being satisfied that transaction is suspicious.

Strict confidentiality will be maintained by the Company and its employees of the fact of furnishing / reporting details of such suspicious transactions.

As advised by the FIU-IND, New Delhi; the Company will not be required to submit 'NIL' reports in casethere are no Cash / Suspicious Transactions, during a particular period.

The required information will be furnished by the Company directly to the FIU-IND, through the designated Principal Officer.

High risk accounts shall be subjected to intensified monitoring. The Company shall set key indicators for such high risk accounts, taking note of the background of the customer, which will include country of origin, source of funds, the type of transactions involved (like accounts having unusual transactions,inconsistent turnover, etc) and other risk factors. Additionally, the Company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligencemeasures basis the revised risk categories.

In addition to the Ordinary Monitoring Standards, any high-risk accounts should also receive the following monitoring:

- Conduct periodic (at least quarterly) reviews of all medium to high-risk accounts
- Create additional reports designed to monitor all transactions in an account to detect patternsof potential illegal activities
- Follow up on any Exceptions detected from the monitoring reports by contacting the account owner personally to inquire about the unusual activity detected and regularly report status of account inquiries to Compliance Officer.

18. RISK MANAGEMENT

I. For effective implementation of KYC policy there will be a proper co-ordination, communication and understanding amongst all the departments of the Company. The Board of Directors shall ensure that an effective KYC program is put in place by establishing proper procedures and ensuring their effectiveimplementation. Heads of all the Departments will ensure that the respective responsibilities in relationto KYC policy are properly understood, given proper attention and appreciated and discharged with utmost care and attention by all the employees of the Company.

II. The Risk department of the Company will carry out quarterly checks to find out as to whether all features of KYC policy are being followed and adhered to by all the Departments concerned. The Risk Department shall sign off on the KYC documents for corporate entities, before every disbursement.

III. The Company shall also mandatorily include KYC adherence in its internal audit scope every quarter. For co-lending partners, the Company shall carry out sample quarterly KYC sample audit by independent audit firms to assess adherence with the KYC norms.

IV. The Company will conduct at regular intervals training programmes to impart training

to its staff members regarding KYC procedures to ensure consistent and highest degree of compliance level.

V. Company shall ensure proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the Company, regulation and related issues.

VI. The inadequacy or absence of KYC standards can subject the Company to serious risks especially reputational, operational, legal and concentration risks.

a. Reputational risk is defined as the risk of loss of confidence in the integrity of the institution,that adverse publicity regarding the Company's business practices and associations, whether accurate or not causes.

b. Operational risk can be defined as the risk of direct and indirect loss resulting from inadequate or failed internal processes, people and systems or from external events.

c. Legal risk is the possibility that law suits, adverse judgments or contracts that turn out to beunenforceable can disrupt or adversely affect the operations or condition of the Company.

d. Concentration risk although mostly applicable on the assets side of the balance sheet, may affect the liability as it is also closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequencesfor the liquidity of the Company.

All these risks are interrelated. Any one of them can result in significant financial cost to the Company and diverts considerable management time and energy to resolving problems that arise.

19. UPDATION / PERIODIC UPDATION OF KYC

Periodic updation shall be carried out at least once in every two years for high-risk customers, once in every eight years for medium risk customers and once in every ten years for low-risk customers from the date of opening of the account / last KYC updation.

20. COMPLIANCE OF KYC POLICY

(a) Entity shall ensure compliance with KYC Policy through:

(i) Specifying as to who constitute 'Senior Management' for the purpose of KYC compliance.
(ii) Allocation of responsibility for effective implementation of policies and procedures.
(iii) Independent evaluation of the compliance functions of entity policies and procedures, including legal and regulatory requirements.
(iv) Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.
(v) Submission of quarterly audit notes and compliance to the Audit Committee.

(b) entity shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

The Company shall ensure compliance with the Master Direction - Know Your Customer (KYC) Direction, 2016, issued and updated from time to time by Reserve Bank of India.

21. POLICY IMPLEMENTATION GUIDELINES

Customer education

For implementing KYC policy, the Company shall have to seek personal and financial

information from the new and intended customers at the time they apply for availing the loan facilities. It is likely that any such information, if asked from the intended customer, may be objected to or questioned by the customers. To meet such situation, it is necessary that the customers are educated and appraised about the sanctity and objectives of KYC procedures so that the customers do not feel hesitant or have any reservation while passing on the information to the Company. For this purpose, all the staff members with whom the customers will have their first interaction / dealing will be provided special training to answer any query or questions of the customers and satisfy them while seeking certain information in furtherance of KYC Policy. To educate the customers and win their confidence in this regard, Companymay arrange printed materials containing all relevant information regarding KYC Policy and anti-moneylaundering measures. Such printed materials will be circulated amongst the customers and in case of any question from any customer, the Company staff will attend the same promptly and provide and explain reason for seeking any specific information and satisfy the customer in that regard.

Introduction of new technologies

As part of the KYC and AML Policy, special attention should be paid to any money laundering threats that may arise from new or developing technologies including on-line transactions that might favour anonymity and adequate measures, if needed, should be taken to prevent their use in money laundering schemes. The Principal Officer should ensure to submit CTR,if any for every month to FIU-IND within the prescribed time schedule.

Applicability to branches and subsidiaries outside India

The KYC and AML Policy will also apply to the branches and majority owned subsidiaries of the Company located abroad, if any. When local applicable laws and regulations prohibit implementation of these guidelines, the same will be brought into the notice of RBI.

KYC policy for existing customers

Although this KYC Policy will apply and govern all the new and prospective customers; some of the KYC procedures laid down in this policy particularly which deal with Customer Identification, Monitoring ofTransactions and Risk Management can be effectively applied to the existing customers and their loanaccounts. While applying such KYC procedures to the existing loan accounts if any unusual pattern is noticed, the same should be brought to the notice of the Department Heads concerned and the Principal Officer appointed by the Company as per RBI directives.

In case any existing customer does not co-operate in providing the information required as per KYC policy or conducts himself in such manner which gives rise to suspicion about his identity or credentials,such matters will be brought to the notice of Principal Officer who in turn will make necessary inquiriesand if required shall forward the name of such customers to the authorities concerned for appropriateaction. Besides above, in such situation the

Company, for reasons to be recorded, may recall the loan granted to such customers and take recourse to legal remedy against the customers as well as security furnished by such customers.

22. APPOINTMENT OF PRINCIPAL OFFICER AND ROLE OF PRINCIPAL OFFICER

Principal Officer is an officer at the management level of the Company and shall be responsible for ensuring compliance, monitoring of transactions, sharing and reporting of information as required under the law/regulations.

Name, designation and address of the Principal officer communicated to the FIU-IND and the RBI.

Role of Principal Officer is defined as under:

➢ The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND;

➢ Utmost confidentiality should be maintained in filing of CTR and STR with FIU-IND. The reports may be transmitted by speed/ registered post, fax, email at the notified address;

➢ It should be ensured that the reports for all the branches are filed in one mode i.e. electronic or manual;

➢ A summary of cash transaction report for the entity as a whole may be compiled by the Principal Officer of the entity in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted both for manual and electronic reporting.

➢ entity is required to initiate urgent steps to ensure electronic filing of cash transaction report (CTR) and Suspicious Transaction Reports (STR) to FIU-IND. In case of NBFCs, where all the branches are not yet fully computerized, the Principal Officer of the NBFC should cull out the transaction details from branches which are not computerized and suitably arrange to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on their website http://fiuindia.gov.in.

entity may not put any restrictions on operations in the accounts where an STR has been made. However, it should be ensured that there is no tipping off to the customer at any level. It is likely that in some cases, transactions are abandoned/ aborted by customers on being asked to give some details or to provide documents. entity should report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

23. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT AND MONITORING OF RISK- ADOPTING RISK BASED APPROACH

Assessment of risk of Money Laundering /Financing of Terrorism helps both the competent authorities and the entity in taking necessary steps for combating ML/FT adopting a risk-based approach. This helps in judicious and efficient allocation of resources and makes the AML/CFT regime more robust. Therefore, entity should carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the entity shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with REs from time to time.

The risk assessment by the entity shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the entity . Further, the periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board of the entity to which power in this regard has been delegated, in

alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated and should be available to competent authorities and self-regulating bodies.

The entity shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on their own or through risk assessment) and should have Board approved policies, controls and procedures in place to effectively manage and mitigate their risk. As a corollary, the entity would be required to adopt enhanced measures for products, services and customers with a medium or high-risk rating.

Indian Banks' Association (IBA) had made an assessment of ML/FT risk in the banking sector. A copy of their Report on Parameters for Risk Based Transaction Monitoring (RBTM) as a supplement to their guidance note on Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards issued in July 2009, is available on the IBA website. The IBA guidance also provides an indicative list of high-risk customers, products, services and geographies. The entity may make use of the same as guidance in their own risk assessment.

In order to have an effective implementation of KYC/AML/CFT measures, the entity would be required to put in place a **system of periodic review of risk categorization of customers and updation of customer identification data in a time-bound manner**.

24. COMBATING FINANCING OF TERRORISM

In terms of PMLA Rules, suspicious repayment transactions should include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism.

The Entity tdeveloped a suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.

As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank circulates these to all banks and financial institutions (including NBFCs). The entity ensure to update the consolidated list of individuals and entities as circulated by Reserve Bank. Further, the updated list of such individuals/entities can be accessed in the United Nations website at http://www.un.org/sc/committees/1267/consolist.shtml.

The entity may note that before opening any new loan account, it should be ensured that the name/s of the proposed customer does not appear in the list.

The entity scaned all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to RBI and FIU-IND.

It may be appreciated that KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking/financial channels. It would,

therefore, be necessary that adequate screening mechanism is put in place by entity as an integral part of their recruitment/hiring process of personnel.

In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, the entity may consider an indicative list of suspicious activities.

25. COUNTRIES WHICH DO NOT OR INSUFFICIENTLY APPLY THE FATF RECOMMENDATIONS

Financial Action Task Force (FATF) has issued several statements on risks arising from the deficiencies in AML/CFT regime of various countries for example Uzbekistan, Iran, Pakistan, Turkmenistan, Sao Tome and Principe on etc. which are updated from time to time.

The entity will consider the information contained in the statements issued by FATF which however, does not preclude financial institutions from legitimate trade and business transactions with the countries and jurisdictions mentioned in the statement.

The entity should take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement. It should, in addition to FATF Statements circulated by Reserve Bank from time to time, also consider publicly available information for identifying such countries, which do not or insufficiently apply the FATF Recommendations. The entity should give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in these countries.

The entity is strictly adhere to the guidelines on KYC/AML/CFT issued from time to time and to those relating to periodical updation of customer identification data after the account is opened and also to monitoring of transactions in order to protect themselves and their customers from misuse by such fraudsters.

The entity is required to ensure that their accounts in banks are not used for the purpose of money laundering in the manner specified above.

26. INTER-GOVERNMENTAL AGREEMENT (IGA) WITH UNITED STATES OF AMERICA (US) UNDER FOREIGN ACCOUNTS TAX COMPLIANCE ACT (FATCA) – REGISTRATION

Government of India has now advised that to avoid withholding tax, Foreign Financial Institutions (FFIs) in Model 1 jurisdictions, such as India, need to register with IRS and obtain a Global Intermediary Identification Number (GIIN) before January 1, 2015. The FFIs who have registered but have not obtained a GIIN should indicate to the withholding agents that the GIIN is applied for, which may be verified by the withholding agents in 90 days. In this regard, the FAQ published on the IRS website (updated as on December 22, 2014), as received from the Government of India, is furnished in the circular DNBR.CC.PD.No.010/03.10.01/2014-15, dated January 9, 2015. Accordingly, the entity may take action appropriately.

27. CONSTITUTION OF SPECIAL INVESTIGATING TEAM – SHARING OF INFORMATION

The Union of India and where needed the State Government will facilitate the conduct of the investigations, in their fullest measures, by the Special Investigation Team and functioning, by extending all necessary financial, material, legal, diplomatic and intelligence resources, whether such investigations or portions of such investigations occur inside the country or abroad.

The entity may extend full co-operation and assistance to the Special Investigation team if required.

Annexure A

Indicative list for Risk Categorization

High Risk

- Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc.;
- Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities;
- Individuals and entities in watch lists issued by Interpol and other similar international organizations;
- Customers with dubious reputation as per public information available or commercially available watch lists;
- Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk;
- Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, etc.;
- Politically exposed persons (PEPs), customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
- Non-face-to-face customers;
- High net worth individuals;
- Firms with 'sleeping partners';
- Companies having close family shareholding or beneficial ownership;
- Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale;
- Shell companies which have no physical presence in branch locations. The existence simply of a local agent or low-level staff does not constitute physical presence;
- Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the Company; - Client Accounts managed by professional service providers such as law firms, accountants, agents,
- brokers, fund managers, trustees, custodians etc.;
- Trusts, charities, NGOs/ unregulated clubs and organizations receiving donations; - Gambling/gaming including "Junket Operators" arranging gambling tours;
- Jewelers and Bullion Dealers; - Dealers in high value or precious goods (e.g. gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers);
- Customers engaged in a business which is associated with higher levels of

corruption (e.g., arms manufacturers, dealers and intermediaries;

- Customers engaged in industries that might relate to nuclear proliferation activities or explosives;
- Customers that may appear to be Multi-level marketing companies etc;
- Individual who is a prisoner in jail

Medium Risk Customers

- Stock brokerage;
- Import / Export
- Gas Station
- Car / Boat / Plane Dealership
- Electronics (wholesale)
- Travel agency
- Telemarketers
- Providers of telecommunications service, internet café, International direct dialing (IDD) call service

Low Risk Customers All other customers (other than High and Medium Risk category) whose identities and sources of wealth can be easily identified and by and large conform to the known customer profile, may be categorized as low risk. In such cases, only the basic requirements of verifying the identity and location of the customer are to be met.