

## **POLICY FRAMEWORK ON "KNOW YOUR CUSTOMER" AND "ANTI-MONEY LAUNDERING MEASURES"**

### **1. OBJECTIVES:**

- To prevent the Company from being used, intentionally or un-intentionally, by criminal elements for money laundering activities.
- To know/understand the Customers and their financial dealings better which, in turn, help in managing their risks prudently.

### **2. KEY ELEMENTS OF THE POLICY:**

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

### **3. DEFINITION OF CUSTOMER:**

- A person or entity that maintains an account and/or has a business relationship with the Company either as a depositor or as a borrower.
- 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 law, and
- Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Company, say, a wire transfer or issue of a high value demand draft as a single transaction

### **4. CUSTOMER ACCEPTANCE POLICY (CAP)**

#### Explicit criteria for acceptance of customers

- No account is opened in anonymous or fictitious / benami name(s)
- Parameters of risk perception are defined in Para 5
- Customers are categorized into different level of risk perception as in Para 5
- Documentation requirements and other information to be collected in respect of different categories of customers depending upon the perceived risk and keeping in mind the requirements of Prevention of Money Laundering Act, 2002.
- Not to open an account or close an existing account where the Company is unable to apply appropriate customer due diligence measures, i.e. unable to verify the identity and /or obtain documents required as per the risk categorization due to non –co-operation of the customer or non reliability of the data/information furnished to the Company
- However, care should be taken that the implementation of the policy does not lead to harassment of the customer,

- Circumstances in which a customer is permitted to act on behalf of another person/entity should be clearly spelt out in the relevant document supporting it, which should be in conformity with the established law and practices.
- Cross Checks should be made to confirm 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.
- The branches will maintain a customer profile as per annexure, containing information relating to the customer's identity, social/financial status, nature of business activity information about client's business and their location, etc.
- This customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

## **5. CATEGORIZATION OF CUSTOMERS ACCORDING TO RISK PROFILE**

### **5.1 LOW RISK CUSTOMERS:**

Customers requiring basic verification of identity and location.

- Salaried employees whose salary structures are well defined
- People belonging to lower economic strata of society whose accounts show small balances and low turn –over
- Government departments and Government owned companies
- Regulators and statutory bodies

### **5.2 MEDIUM RISK CUSTOMERS**

- Non-Resident customers
- High Net-Worth individuals
- Trusts, Charities, Non-Government Organizations (NGO) and organizations receiving donations
- Companies having close family shareholding or beneficial ownership
- Firms with ' sleeping partners'

### **5.3 HIGH RISK CUSTOMERS**

Customers requiring thorough probe

- Politically Exposed Persons (PEP) of foreign origin
- Non-face to face customers
- Those with dubious reputation as per public information available

The categorization of customers as per risk profile and implementation of the measures, however, should not result in denial of Company's services to general public, especially to those, who are financially or socially disadvantaged.

## **6. CUSTOMER IDENTIFICATION PROCEDURE**

As per the Rule 9 of 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 (PML Rules) requires that our Company:

- At the time of commencement of an account-based relationship, identify its customers, verify identity and obtain information on the purpose and intended nature of business relationship.

Customer Identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information.

- Customer Identification Procedure will be carried out at different stages as follows:
- While establishing a relationship
- Transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transaction that appear to be connected, or
- Any international money transfer operations

When the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data, company may further demand data as follows:

- For customers that are natural persons, sufficient identification data to verify the identity of the customer, his address/location and also his recent photograph.
- For Customers that are legal persons or entities, the legal status of the legal person/entity should be verified through proper and relevant documents. For any person purporting to act on behalf of the legal person/entity, it has to be verified whether he is so authorized and his identification has to be verified. Also, the ownership and control structure of the customer should be understood so as to determine who are the natural persons who ultimately control the legal person.
- Customer identification requirements in respect of a few typical cases, especially legal persons requiring an extra element of caution are given in **Annexure – 1**.
- An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in **Annexure – 2**.

## **7. MONITORING OF TRANSACTIONS:**

- Ongoing monitoring is an essential element of effective KYC procedures.
- Special attention will be paid to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.
- The Branches will have to regularly monitor the transactions of over Rs.10 lakh.
- The monitoring will be done according to the Risk level of the borrowers and any abnormal transaction will have to be probed.
- A record of such transactions which are inconsistent with the level of the borrowers and also transactions of suspicious nature will be maintained at the branch in terms of Section 12 of Prevention of Money Laundering Act, 2002.
- Any cash transaction of over Rs.10 lakh and also of any suspicious nature has to be reported by the branches to Registered Office of the Company on a monthly basis in the following format. If no transaction of such nature has taken place, the branch should report 'nil' statement to Registered Office.

Name of the Account

Date of transaction

Amount involved

Remarks

**8. RISK MANAGEMENT**

- All branches will strictly comply with the laid down policies on Accounting, Lending, Recovery, etc., and also the guidelines issued from Registered Office from time to time.
- The auditors auditing the branches will thoroughly check the application of KYC norms in the branches and comment on the lapses observed in this regard. Compliance on KYC norms by branches will be put before the Audit Committee at regular intervals.
- Registered Office will ensure that all the frontline staff members are kept informed well of the KYC norms and procedures for implementation.

**9. CUSTOMER EDUCATION**

- Registered Office will be providing specific literature/pamphlets to educate the customers on the objectives of KYC norms and procedures seeking their cooperation in getting the information required from them.

**10. INTRODUCTION OF NEW TECHNOLOGIES:**

- Registered Office will ensure that necessary control mechanism will be built in the Software packages to be implemented in the branches to prevent the use of the technology for money laundering purposes

**11. KYC FOR THE EXISTING ACCOUNTS:**

- The Branches will apply the KYC norms to the existing customers on the basis of materiality and risk. Transactions in existing accounts will be continuously monitored and any unusual pattern will be reviewed by the branch manager.
- The existing term deposit accounts will be treated as new accounts at the time of renewal and KYC norm will be applied.
- In spite of the best efforts on its part, if the branch is unable to get the desired information from the account holder due to his non-cooperation, the branch should consider closing the account and terminate the business relationship after issuing notice to the customer explaining the reasons for taking such a decision and recommend the closure of the account to Registered Office, who will advise the branch accordingly / suitably.

**12. APPOINTMENT OF PRINCIPAL OFFICER:**

- General Manager of the Company at Registered Office will be Principal Officer of the Company to coordinate the implementation of KYC norms in the Company.
- The Principal Officer is authorized to fix the accountability for serious lapses and intentional circumvention of prescribed procedures and guidelines, in consultation with the Managing Director of the Company.

**13. MAINTENANCE OF RECORDS OF TRANSACTIONS:**

- All branches will be maintaining proper record of transactions prescribed under Rule 3 of the Prevention of Money Laundering Act, 2002 as mentioned below:
- All cash transactions of the value of more than Rs.10 lakh or its equivalent in foreign currency.

- All series of cash transactions integrally connected to each other which have been valued below Rupees ten lakh where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh.
- All transactions involving receipts by non-profit organizations of rupees ten lakh or its equivalent in foreign currency,
- 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
- All suspicious transactions whether or not made in cash and by way of as mentioned in the rules.
- The branches are required to maintain proper record of all cash transactions of Rs.10 lakhs and above. Further, all such transactions/suspicious transactions whether made in cash or other wise, to be reported to Registered Office by the branches, on fortnightly basis.
- The branches are required to maintain the following information in respect of transactions referred to Rule 3 of the prevention of Money Laundering.
  - i) the nature of 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. MAINTENANCE AND PRESERVATION OF RECORDS**

- The branches will maintain the records for at least 10 years from the date of cessation of transaction between the bank and the client so as to retrieve the transactions and provide evidence for prosecution of persons involved in criminal activity.
- All branches will maintain the records pertaining to the identification of the customers and their addresses including copies of passports, identity card, driving licenses, pan, utility bills, obtained while opening the account and during the course of business relationship and properly preserve for at least 10 years after the business relationship is ended. The identification records and transaction data should be made available to the competent authorities upon request.

#### **15. REPORTING TO FINANCIAL INTELLIGENCE UNIT – INDIA**

- The Company will be reporting the information in the proper format, transactions relating to cash and suspicious nature to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND  
 Financial Intelligence Unit – India  
 6<sup>th</sup> Floor, Hotel Samrat  
 Chanakyapuri  
 New Delhi – 110 021

1. The information in respect of the transactions referred to in clause (A), (B) and (BA) of sub-rule (1) of rule 3 of the PML Rules (i.e. clauses mentioned in para 13 above) is to be submitted to the Director every month by the 15<sup>th</sup> day of succeeding month. (Annexure 3-10)

2. The information to be submitted to the Director promptly, in writing or by E-mail, or by fax, not later than seven working days from the date of occurrence of such transaction and on being satisfied that the transaction is suspicious. (As per Annexure 3-10)

## **16. On-going Due Diligence**

1. On-going due diligence of customers should be done to ensure that transactions are consistent with the knowledge about the customers, customers' business and risk profile; and the source of funds.
2. Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:
  - a. Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
  - b. Transactions which exceed the thresholds prescribed for specific categories of accounts.
  - c. High account turnover inconsistent with the size of the balance maintained.
  - d. Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

3. The extent of monitoring shall be aligned with the risk category of the customer.

Explanation: High risk accounts have to be subjected to more intensified monitoring.

- a. A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.
- b. The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

Explanation: Cases where a large number of cheque books are sought by the company and/or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.

## **4. Periodic Updation:**

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 as per the following procedure:

- a. All Branches shall carry out:
  - i. PAN verification from the verification facility available with the issuing authority and
  - ii. Authentication, of Aadhaar Number already available with the RE with the explicit consent of the customer in applicable cases.
  - iii. In case identification information available with Aadhaar does not contain current address an OVD containing current address may be obtained.
  - iv. Certified copy of OVD containing identity and address shall be obtained at the time of periodic updation from individuals not eligible to obtain Aadhaar, except from individuals who are categorised as 'low risk'. In case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.
  - v. In case of Legal entities, RE shall review the documents sought at the time of opening of account and obtain fresh certified copies.
- b. Branches may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, OVD/Consent forwarded by the customer through mail/post, etc., shall be acceptable.

- c. Branches shall provide acknowledgment with date of having performed KYC updation.
- d. The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

---

## **ANNEXURE - 1**

### **CUSTOMER IDENTIFICATION REQUIREMENTS INDICATIVE GUIDELINES**

#### **1. Trust/Nominee or Fiduciary Accounts:**

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Branches should determine whether the customer is acting on behalf another person as trustee/nominee or any other intermediary. If so, the Branch may insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for trust, the branches should take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a "foundation" steps should be taken to verify the founder managers/directors and the beneficiaries, if defined.

#### **2. Accounts of Companies and firms**

The branches need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with the branches. The branches should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perceptions, e.g. in the case of a public company it will not be necessary to identify all the shareholders.

#### **3. Client accounts opened by professional intermediaries:**

When the Branch has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. The Branches may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Where the branches rely on the 'customer due diligence' done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It should be understood that the ultimate responsibility for knowing the customer lies with the branch.

#### **4. Accounts of Politically Exposed Persons (PEPs) resident outside India**

Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g. Heads of States or of Governments senior politicians, senior Government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Branches should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person and seek information about the sources of funds before accepting PEP as a Customer. The decision to open an account for PEP should be taken at a senior level above the category of the concerned branch manager. Branches should monitor such accounts on an ongoing basis. These norms are also applicable to the accounts of the family members or close relatives of PEPs.

#### **5. Accounts of non-face-to-face customers:**

In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the branch may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

**ANNEXURE - 2**

**CUSTOMER IDENTIFICATION PROCEDURE FEATURES TO BE VERIFIED AND DOCUMENTS THAT MAY BE OBTAINED FROM CUSTOMERS**

Customers/Clients	Documents
<p><b>For Individuals</b></p> <p>-Proof of Identity and Address</p>	<p>(i) Passport</p> <p>(ii) PAN card</p> <p>(iii) Voter's Identity Card</p> <p>(iv) Driving License</p> <p>(v) Job Card issued by NREGA duly signed by an officer of the State Govt</p> <p>(vi) The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number.</p> <p>For verifying for the limited purpose of proof of address the following additional documents are deemed to be OVDs :</p> <ol style="list-style-type: none"> <li>I. Utility bill which is not more than two months old of any service provider (electricity, telephone, postpaid mobile phone, piped gas, water bill);</li> <li>II. Property or Municipal Tax receipt;</li> <li>III. Bank account or Post Office savings bank account statement;</li> <li>IV. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;</li> <li>V. Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and</li> <li>VI. Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India.</li> </ol>
<p><b>For Companies</b></p> <p>-Name of the Company</p> <p>-Principal place of business</p> <p>-Mailing address of the Company</p> <p>-Telephones/Fax number</p>	<ol style="list-style-type: none"> <li>i. Certificate of Incorporation and Memorandum and Articles of Association</li> <li>ii. Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account.</li> <li>iii. Power of Attorney granted to its managers, officers or employees to transact the business on its behalf</li> <li>iv. Copy of PAN allotment letter</li> <li>v. Copy of the telephone bill</li> </ol>
<p><b>For Partnership firms</b></p> <p>-Legal Name</p> <p>-Address</p>	<ol style="list-style-type: none"> <li>i. Registration certificate, if registered</li> <li>ii. Partnership deed</li> <li>iii. Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf</li> <li>iv. Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses</li> </ol>

<p>-Name of all the partners and their addresses</p> <p>- Telephone numbers of the firm and partners</p>	<p>v. Telephone Bill in the name of firm and/partners</p>
<p><b>For Trusts &amp; Foundations</b></p> <p>-Names of trustees, settlers, beneficiaries and signatories</p> <p>-Name and Addresses of the founder, the managers/directors and the beneficiaries</p>	<p>i. Certificate of registration, if registered</p> <p>ii. Power of Attorney granted to transact business on its behalf</p> <p>iii. Any officially valid document to identify trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/directors and their addresses</p> <p>iv. Resolution of the managing body of the foundation/association</p> <p>v. Telephone Bill</p>
<p><b>For Unincorporated association or a body of individuals</b></p>	<p>i. Resolution of the managing body of such association</p> <p>ii. Power of attorney granted to him to transact on its behalf,</p> <p>iii. an officially valid document in respect of the person holding an attorney to transact on its behalf,</p> <p>iv. any such other information as branch may require collectively to establish the legal existence of such association or body of individuals.</p>

## **Manual Reporting Formats (Annexure 3 to 10)**

1. Manual cash transaction report – Annexure -3
2. Manual Cash transaction report- Individual detail sheet – Annexure -4
3. Manual Cash transaction report – Legal person/entity detail sheet – Annexure-5
4. MCTR(S) Summary of Manual Cash Transaction Reports for HFCs – Annexure-6
5. MSTR (Manual Suspicious Transactions Report) for HFCs – Annexure-7
6. MSTR(IDS) – Annexure-A (Manual Suspicious Transactions Report – Individual detail sheet) – Annexure-8
7. MSTR (LP/Entity-Details) – Annexure-B (Manual Suspicious Transaction Report – Legal persons/Entity) Annexure-9
8. MSTR(ADS) – Annexure-C (Manual Suspicious Transaction Report – Account Details Sheet) – Annexure-10
9. Illustrative (but not exhaustive) list of suspicious transactions in housing/builder/project loans

### **II. ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTIONS PERTAINING TO BUILDER/PROJECT LOANS :**

- a. Builder approaching the HFC for a small loan compared to the total cost of the project.
- b. Builder is unable to explain the sources of funding for the project.
- c. Approvals/sanctions from various authorities proved to be fake.

## **Annexure-11**

### **I. ILLUSTRATIVE LIST OF SUSPICIOUS TRANSACTIONS PERTAINING TO HOUSING LOANS :**

- a. Customer is reluctant to provide information, data, documents;
- b. Submission of false documents, data, purpose of loan, details of accounts;
- c. Refuses to furnish details of source of funds by which initial contribution is made, sources of funds is doubtful, etc;
- d. Reluctant to meet in person, represents through a third party/Power of Attorney holder without sufficient reasons;
- e. Approaches a branch/office of a HFC, which is away from the customer's residential or business address provided in the loan application, when there is HFC branch/office nearer to the given address;
- f. Unable to explain or satisfy the numerous transfers in the statement of account/multiple accounts;
- g. Initial contribution made through unrelated third party accounts without proper justification;
- h. Availing a top-up loan and/or equity loan, without proper justification of the end use of the loan amount;
- i. Suggesting dubious means for the sanction of loan;
- j. Where transactions do not make economic sense;
- k. There are reasonable doubts over the real beneficiary of the loan and the flat to be purchased;
- l. Encashment of loan amount by opening a fictitious bank account;
- m. Applying for a loan knowing fully well that the property/dwelling unit to be financed has been funded earlier and that the same is outstanding;
- n. Sale consideration stated in the agreement for sale is abnormally higher/lower than what is prevailing in the area of purchase;
- o. Multiple funding of the same property/dwelling unit;
- p. Request for payment made in favour of a third party who has no relation to the transaction;
- q. Usage of loan amount by the customer in connivance with the vendor/ builder/ developer/ broker/ agent, etc. and using the same for a purpose other than what has been stipulated;
- r. Multiple funding/ financing involving NGO/ Charitable Organisation/ Small/Medium Establishments (SMEs) / Self Help Groups (SHGs) / Micro Finance Groups (MFGs);
- s. Frequent requests for change of address;
- t. Overpayment of instalments with a request to refund the overpaid amount.