Know Your Customers Guidelines

The Reserve Bank of India (RBI) has issued guidelines on 'Know Your Customer' (KYC) Guidelines – Anti Money Laundering Standards for Non Banking Finance Companies (NBFCs) thereby setting standards for prevention of money laundering activities and corporate practices while dealing with their customers. The Company shall adopt all the best practices prescribed by RBI from time to time and shall make appropriate modifications if any necessary to this Code to conform to the standards so prescribed.

This policy is applicable across all branches /business segments of the company, and its financial subsidiaries and is to be read in conjunction with related operational guidelines issued from time to time. The contents of the policy shall always be read in tandem/auto-corrected with the changes/modifications which may be advised by RBI from time to time.

For the purpose of KYC policy, a 'Customer' may be defined as:

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

Objective:

The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable the Company to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. The Company hereunder framing its KYC policies incorporating the following four key elements:

(i) Customer Acceptance Policy
(ii) Customer Identification Procedures;
(iii) Monitoring of Transactions; and
(iv) Risk management.

(i) Customer Acceptance Policy (CAP)

The guidelines for Customer Acceptance Policy (CAP) for the company are given below:

- No account is opened in anonymous or fictitious/ benami name(s).
- The company shall classify customers into various risk categories and based on risk perception decide on acceptance criteria for each customer category.
- Accept customers after verifying their identity as laid down in customer identification procedures.
- While carrying out due diligence the company will ensure that the procedure adopted will not result in denial of services to the genuine customers.
- For the purpose of risk categorisation of customer, company shall obtain the relevant information from the customer at the time of account opening.

(ii) Customer Identification Procedure (CIP)

The policy approved by the Board of the Company clearly spell out the Customer Identification Procedure to be carried out at different stages i.e. while establishing a business relationship; carrying out a financial transaction or when the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data. Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. The Company will obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of business relationship. Being satisfied means that the Company must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based approach is considered necessary to avoid disproportionate cost to Company and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc).

For customers that are natural persons, the Company will obtain 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 bank will (i) verify the legal status of the legal person/ entity through proper and relevant documents (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person, (iii) understand the ownership and control structure of the customer and 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-I for guidance of Company.

The Company has framed its own internal guidelines based on their experience of dealing with such persons/entities, normal lender's prudence and the legal requirements as per established practices. The Company will take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are. An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in the Annexure-I. Documentation requirements and other information shall be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Reserve Bank of India from time to time.

Necessary checks wherever and to the extent possible, shall be conducted before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities.

The documents requirements would be reviewed periodically as and when required for updation keeping in view the emerging business requirements. Senior Official(s) in charge of the Policy are empowered to make amendments to the list of such documents required for customer identification in consultation with the sales and distribution channels and compliance.

Customer Identification Procedure is to be carried out at different stages i.e.

- while establishing a business relationship (or)
- carrying out a financial transaction (or)
- where the company has a doubt about the authenticity/veracity (or)
- Inadequacy of the previously obtained customer identification data if any.
- When the company feels it is necessary to obtain additional information from the existing customers based on the conduct or behaviour of the account.

No deviations or exemptions shall normally be permitted in the documents specified for account opening. In case of any extreme cases of exceptions, concurrence of Policy section should be obtained duly recording the reasons for the same. Suitable operating guidelines for implementation of the KYC/ AML guidelines shall be issued by the company for its different business segments.

(iii) Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity attached with the client. The Company will pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

The Company may prescribe threshold limits for a particular category of clients and pay particular attention to the transactions which exceed these limits. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer would particularly attract the attention of the Company.

The Company ensures that its branches continue to maintain proper record of all cash transactions. The internal monitoring system will have an inbuilt procedure for reporting of such transactions and those of suspicious nature to controlling/ head office on a fortnightly basis.

Section 3 of the Prevention of Money Laundering (PML) Act 2002 has defined the "offence of money laundering" as under:

"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering".

All transactions of suspicious nature shall be reported. The Principal Officer of the Company shall ensure that such reporting system is in place and shall monitor receipt of the reports. All transactions of suspicious nature and/ or any other type of transaction notified under section 12 of the PML Act, 2002, shall be reported to the appropriate law enforcement authority by the Principal Officer. The necessary documents, information and records would be maintained and preserved for the period prescribed under AML Act would be maintained.

(iv) Risk Management

The Board of Directors of the Company ensures that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It will cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility would be explicitly allocated within the Company for ensuring that the Company's policies and procedures are implemented effectively. The Company may, in consultation with their boards, devise procedures for creating Risk Profiles of their existing and new customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

The Company's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function provides an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. The Company ensure that its audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Concurrent/ Internal Auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard may be put up before the Audit Committee of the Board on quarterly intervals.

The Company have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements will have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

Appointment of Principal Officer

The Company amongst its senior management officers, shall appoint one officer to be designated as Principal Officer. Principal Officer shall be located at the head office of the Company and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

Annexure - I

Customer Identification Procedure Features to be verified and documents that may be obtained from customers

Individuals: Legal name and any other names used – Correct permanent address

Companies - Name of the company - Principal place of business - Mailing address of the company - Telephone/Fax Number

Partnership firms Legal name - Address Names of all partners and their addresses – Telephone numbers of the firm and partners

Trusts & foundations - Names of trustees, settlers, beneficiaries and Signatories Names and addresses of the founder, he managers /directors and the Beneficiaries - Telephone / fax numbers

Documents

For Individuals: (I) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving licence (v) Identity card (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of bank (i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority (iv) Electricity bill (v) Ration card (vi) Letter from employer (any one document which provides customer information)

For Companies: (i) Certificate of incorporation and Memorandum & Articles of Association (ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf (iv) Copy of PAN allotment letter (v) Copy of the telephone bill

For Partnership Firms: (I) Registration certificate, if registered (ii) Partnership deed (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (iv) Any officially valid document identifying the Partners and the persons holding the Power of Attorney and their addresses (v) Telephone bill in the name of firm/partners

For Trusts & Foundation: (i) Certificate of registration, if registered (ii) Power of Attorney granted to transact Business on its behalf (iii) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/ Directors and their addresses (iv) Resolution of the managing body of the foundation / association (v) Telephone bill