Know Your Customer

6th November 2019

Know Your Customer

Introduction:

KYC (Know Your Customer) is the platform on which the company operates to avoid shortcomings in operational, legal and reputation risks to the institution and the consequential losses by scrupulously following various procedures laid down for opening and conduct of accounts. Money laundering is involvement in any transaction or series of transactions seeking to conceal or disguise the nature or source of proceeds derived from illegal activities including drug trafficking, armed robbery, tax evasion, smuggling, etc. KYC guidelines are accepted internationally as an important anti-money laundering measure.

In compliance with the guidelines issued by RBI from time to time, the following AML & KYC policy of the Company is approved by the Board of Directors of the Company.

Objectives:

AML Policy

The primary objective of the policy is to prevent the company from being used intentionally/ unintentionally by criminal elements for money laundering or terrorist financing activities. The policy seeks:

i. To prevent the criminals from using the company for money laundering activities
ii. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with the applicable laws and laid down procedures
iii. To promote compliance with laws pertaining to financial sector
iv. To eliminate the risk that the company will be used for illicit or illegal activities
v. To reduce the risk of government seizure and forfeiture of a client's loan collateral when the customer is involved in criminal activity
vi. To protect the company's reputation
vii. To check misappropriations
viii. To weed out undesirable customer
ix. To avoid opening of accounts with fictitious names and addresses
x. To monitor transactions of suspicious nature

xi. To ensure that employees of the company are adequately trained in KYC/ AML/ CFT procedures.

Definition of Money Laundering:

Section 3 of Prevention of Money Laundering Act (PMLA) defines "the offence of money laundering" as follows:

"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". The process involves creating a web of financial transactions so as to hide the true nature and origin of funds. For the purpose of this policy, the term money laundering would also cover financial transactions where the end use of funds goes for terrorist financing irrespective of the source of the funds.

Obligations of PMLA:

Section 12 of PMLA requires every financial intermediary

To maintain a record of prescribed transactions

To furnish information of prescribed transactions to the specified authority

To verify and maintain records of the identity of its clients

To preserve records in respect of the above for a period of ten years from the date of cessation of the transactions with the clients.

"Suspicious transaction" means a transaction including an attempted transaction, whether or not made in cash, which to a person acting in good faith;

(a) Gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the schedule to the Act, regardless of the value involved; or
(b) Appears to have no economic rationale or bonafide purpose; or
(c) Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Key Elements of the KYC Policy

KYC Policy includes the following nine key elements:

1. Customer Acceptance Policy (CAP)

2. Customer Identification Procedures (CIP)

3. Monitoring of Transactions
4. Risk management
5. Training Programme
6. Internal Control Systems
7. Record Keeping
8. Assessment and Review
9. Duties / Responsibilities and Accountability
10. Periodical updating of customer identification data of existing customers" could also be included

1. Customer Acceptance Policy:

It lays down the criteria for acceptance of customers. The guidelines in respect of the customer relationship are as follows:

i. No account is to be opened in anonymous or fictitious/benami name(s)/entity (ies)
ii. Accept customers only after verifying their identity, as laid down in Customer Identification Procedures.
iii. Classify customers into various risk categories and, based on risk perception, apply the acceptance criteria for each category of customers. Also, a profile of each customer will be prepared based on risk categorization
iv. Documentation requirements and other information to be collected, as per PMLA and RBI guidelines/instructions, to be complied with
v. Not to open an account or close an existing account (except as provided in this Policy), where identity of the account holder cannot be verified and/or documents/information required could not be obtained/confirmed due to non-cooperation of the customer
vi. Identity of a new customer to be checked so as to ensure that it does not match with any person with known criminal background or banned entities such as individual terrorists or terrorist organizations available from circulars etc.
vii. The decision to open an account for Politically Exposed Person (PEP) should be taken at a senior level. It may, however, be necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision to close an account may be taken at a reasonably high level after giving due

notice to the customer explaining the reasons for such a decision.

viii. Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be strictly followed.

CAP requirements for various categories of customers:

A.TRUST/NOMINEE OR FIDUCIARY ACCOUNTS

Branch/offices should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, branch/offices 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 a trust, branches/offices 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', branches should take steps to verify the founder managers/directors and the beneficiaries, if defined. There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures.

B.ACCOUNTS OF COMPANIES AND FIRMS

Branch/office need to be vigilant against business entities being used by individuals as a front for maintaining accounts with the company. Branch/ office may 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 perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

C.CLIENT ACCOUNTS OPENED BY PROFESSIONAL INTERMEDIARIES

When the Branch/office 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. Branch/office may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Branch/office also maintains „pooled' accounts managed by lawyers/ chartered accountants for funds held „on deposit' for a range of clients. Where funds held by the intermediaries are not co-mingled at the Branch/office and

there are 'sub-accounts', each of them attributable to beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the Branch/office, the company should still look through to the beneficial owners. Where the Branch/ office rely on the 'customer due diligence' (CDD) means identifying and verifying the customer and the beneficial owner 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/office.

D.ADHERENCE TO FOREIGN CONTRIBUTION REGULATION ACT (FCRA), 1976

Branches/Offices should also adhere to the instructions on the provisions of the Foreign Contribution Regulation Act, 1976 cautioning them to open accounts or collect cheques only in favour of association, which are registered under the Act ibid by Government of India. A certificate to the effect that the association is registered with the Government of India should be obtained from the concerned associations at the time of opening of the account or collection of cheques. Branches/offices are advised to exercise due care to ensure compliance and desist from opening accounts in the name of banned organizations and those without requisite registration.

E.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. Branch/office 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 in the public domain. Branch/office should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for PEP should be taken at a senior level and should be subjected to monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs

Category based Customer Profile:

Branches/offices should prepare a profile for each new customer based on risk categorization. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients, business and their location etc.

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

Customers that are likely to pose a higher than average risk maybe categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Enhanced due diligence measures are to be applied 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.

2. Customer Identification Procedures (CIP):

Obtaining Customer identification requires identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Thus, the first requirement of Customer Identification Procedures (CIP) is to be satisfied that a prospective customer is actually who he/she claims to be. The second requirement of CIP is to ensure that sufficient information is obtained on the identity and the purpose of the intended nature of the customer relationship. This would enable risk profiling of the customer and also to determine the expected or predictable pattern of transactions. Identification data that would be required to be obtained for various classes of customers are as below:

NATURAL PERSON

- Address/ location details
- Recent photograph

LEGAL PERSONS

A. Legal status of the legal person/entity through proper and relevant documents.

B. Verification that any person purporting to act on behalf of the legal person/entity is so authorized and identity of that person/entity is established and verified.

C. Understand the ownership and control structure of the customer and determine who are natural persons who, ultimately control the legal person. Wherever applicable, information on the nature of business activity, location, mode of payments, volume of turnover, social and financial status etc. will be collected for completing the profile of the customer.

D. If the branch/office decides to accept such accounts in terms of the Customer Acceptance Policy, the company should 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.

D.NEW ACCOUNTS

"Know Your Customer" (KYC) procedure should be the key principle for identification of an individual/corporate opening an account. The customer identification should entail verification through an employee of the company and on the basis of documents provided by the customer. The objectives of the KYC framework shall be two-fold:

- To ensure appropriate customer identification
- To monitor transactions of a suspicious nature

Branches/offices should obtain all information necessary to establish the identity/legal existence of each new customer, based preferably on disclosures by customers themselves. Easy means of establishing identity would be documents such as passport, driving license, etc. The Company shall also ensure personal verification by the employee of the company.

ACCEPTABLE DOCUMENTS

Identity Proof

Individual:

Valid Passport
Voter identity card issued by Election Commission of India
Valid PAN card
Valid driving license
Job card issued by NREGA duly signed by an officer of the State

Government
Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.

Others:

Company:

Certification of incorporation
MOA/AOA
Resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf

Partnership Firms:

Registration certificate
Partnership deed
An officially valid document in respect of the person holding an attorney to transact on its behalf.

Trust and Foundations:

Registration certificate
Trust deed
An officially valid document in respect of the person holding an attorney to transact on its behalf.

Unincorporated association or body of individuals:

Resolution of the managing body of such association or body of individuals
Power of attorney granted to him to transact on its behalf
An officially valid document in respect of the person holding an attorney to transact on its behalf.
Such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals

Address Proof

Individuals:

Valid passport

Voter identity card issued by Election Commission of India
Valid driving license,
Job card issued by NREGA duly signed by an officer of the State Government
Letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.

Others:

Company:

Certification of incorporation
MOA/AOA
Resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf

Partnership Firms:

Registration certificate
Partnership deed
An officially valid document in respect of the person holding an attorney to transact on its behalf.

Trust and Foundations: - Registration certificate

Trust deed
An officially valid document in respect of the person holding an attorney to transact on its behalf.

Unincorporated association or body of individuals:

Resolution of the managing body of such association or body of individuals
Power of attorney granted to him to transact on its behalf
An officially valid document in respect of the person holding an attorney to transact on its behalf.
Such information as may be required by the bank to collectively establish the legal existence of such an association or body of individual

Proprietary Concerns

For proprietary concerns, the company should call for and verify any two of the following documents:

Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/licence

issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST / VAT certificate, certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, etc.

Any registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority / Department. NBFCs/RNBCs may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of account.

The complete Income Tax return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/ acknowledged by the Income Tax Authorities.
- Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern.

E. **Customer profile:**

The company while evaluating a prospective customer obtains important information like the customer's source of funds, source of income and assets, etc. through collection of following details:

a. Details of employment/ business/ vocation or profession

b. Details of income and annual income

c. Details of assets owned, such as house, vehicle, etc.

d. Other personal details such as qualification, marital status

e. Dealings with banks/ other financial institutions and the credit history Drawing up of customer profile would give an idea as to the nature and volume of transactions/ activities to expect in the account as assessed/ envisaged at the time of opening of an account. If the transactions are in variance with the profile of client, the customer should be contacted for further details to the satisfaction of the company.

F. <u>Reliance on third party due diligence:</u>

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

a. the Company obtains necessary information of such client due diligence carried out by the third party;
b. the Company 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;

c. the Company 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 Act;
d. the third party is not based in a country or jurisdiction assessed as high risk; and
e. the Company is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

G. Risk Categorization of Customers

The Company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Such review of risk categorization of customers will be carried out at a periodicity of not less than once in six months.

The Company shall have a system in place for periodical updation of customer identification data after the account is opened. Full KYC exercise will be done at a periodicity not less than once in ten years in case of low risk category customers, not less than once in eight years in case of medium risk category customers and not less than once in two years in case of high-risk category customers.

Low Risk Category

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, shall be categorised as low risk.

Illustrative examples are:

1. Salaried employees whose salary structure is well-defined
2. People belonging to lower economic strata of the society whose accounts show small balances and low turnover
3. Government departments and Government-owned companies
4. Statutory bodies & Regulators
5. Self – employed individuals / Proprietary Firms / Hindu Undivided Families (HUFs)
6. Limited Companies (Public and Private)
7. Partnership Firm with registered deed.

Medium & High-Risk Category

Customers that are likely to pose a higher than average risk may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc.

Illustrative examples of medium risk category customers are:

1. Non-Resident customers
2. Trust, charities, NGO's and Organization receiving donations

Illustrative examples of high-risk category customers are:

1. Politically Exposed Persons (PEPs) of Indian/Foreign Origin
2. Those with dubious reputation as per public information available

H. Photographs:

At the time of evaluating the proposal, two passport size photographs of each borrower and guarantor should be obtained which are self-attested.[1] Where the borrower and/or guarantor are an artificial person, photographs of directors/ partners/ Karta as the case may be, need to be obtained which are self-attested.[2]

I. Field Inspection:

As part of proposal evaluation process, an employee of the company visits the office and/or residential address of the customer to verify the claims made in the loan application form and meets the borrower to address doubts, if any.

3. Monitoring of Transactions:

Ongoing monitoring is an essential element of effective KYC procedures. Branches 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 of the account.

Branches should pay special attention to all complex, unusually large transactions and all unusual patterns, which have no apparent economic

[1] Ibid

[2] Ibid

or visible lawful purpose. The branch/office may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions, which exceed these limits. High-risk accounts have to be subjected to intensify monitoring. The company should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors.

Branches are required to record and report all transactions of suspicious nature in deposit, loan and remittance accounts etc, with full details to their controlling Offices. The Principal officer/Officer -in charge, vested with the authority to open the account, is to ensure compliance with the KYC guidelines. The employee/officer, who has interviewed the customer's to subscribe his signature for having interviewed the prospective customer and the officer before permitting opening of the account, to satisfy that all aspects of KYC guidelines are complied with.

Reporting of Suspicious Transactions:

To observe four eyes concept in reporting suspicious transactions at branch level, first dealing officer at the branch will report to the Branch Manager (BM), who will get himself satisfied about existence of a suspicious activity/nature and then report to the controlling office. Further course of action is to be recommended by the controlling officer in consultation with Law Department to H.O. The designated officer at H.O has to take up the matter with appropriate law enforcing authorities designated under the relevant laws governing such activities.

Terrorist Finance:

In case the name of any banned organization is noticed as payee/endorsee/applicant, the first dealing officer shall report the same to the Principal Officer. Reporting of such transactions as and when detected is to be done as under:

Reporting by	**Reporting to**
1. Branch	1. Controlling office
2. Controlling office	2. Principal Officer (PO). H.O.
3 .PO/. H.O	3.FIU - IND

All cash transactions, where forged or counterfeit Indian currency notes have been used, shall also be reported immediately by the branches, by way of Counterfeit Currency Reports (CCRs) to the Principal Officer, through proper channel, for onward reporting to FIU-IND.

4. Risk Management

The company has put in place an effective KYC programme in place by establishing appropriate procedures and ensuring their effective implementation covering proper management oversight, systems and controls, segregation of duties, training and other related matters.

Responsibility has also been explicitly allocated within the company for ensuring that the company's policies and procedures are implemented effectively. The nature and extent of due diligence will depend on the risk perceived by the branch/company. However, while preparing customer profile branches should take care to seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

The company's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The compliance function should provide an independent evaluation of the company's own policies and procedures, including legal and regulatory requirements. It would be ensured that the audit machinery is staffed adequately with individuals who are well versed in such policies and procedures. Head – Credit is the principal officer for monitoring Anti Money Laundering Issues. A dedicated credit audit team under the direct supervision of Head - Credit checks and confirms compliance with the KYC policies and procedures in respect of all the loan contracts.

5. Training of Employees:

As part of induction process, employees across the country are trained in KYC guidelines through online training module. Updation and modifications, if any, in the guidelines are also cascaded to the entire team to keep them abreast of the changes

6. Internal Credit controls and Internal Audit:

Head is the nodal officer for monitoring Anti Money Laundering issues like review of transactions of suspicious nature and verifying compliance of guidelines in this regard. KYC/AML guidelines are inbuilt into the Standard Operating Procedure by designating a maker checker & reviewer for each activity. The location in charge / executive verifies the original document of the borrower and endorses "Original Seen and Verified" in every document. The Hub Credit Administrator (HCA) checks and confirms if the above documents are in place before the disbursal of the loan. The Credit Quality Compliance team at RMC reviews the entire file.

7. Record Keeping:

As per the guidelines of Reserve Bank of India, the company is required to prepare and maintain documentation on their customer relationships and transactions to meet the requirements of relevant laws and regulations and to enable any transactions effected through them to be reconstructed. All financial transactions records are required to be retained for at least 10 years after the transaction has taken place and should be available for perusal and scrutiny of audit functionaries as well as regulators as and when required.

8. Assessment and review:

The Company shall also undertake periodic (at least annual) assessment of KYC/AML policies and procedures to ensure that compliance functions continue to function effectively.

9. Principal / Nodal Officer:

Head - Credit

Hinduja Leyland Finance Limited No. 27A, Developed Industrial Estate
Guindy, Chennai – 600032

Phone: +91 44 22427526

Email: compliance@hindujaleylandfinance.com

10. Designated Director:

The Board at its meeting held on 24th January, 2017 had nominated Mr. S. Nagarajan, whole-time director as the designated director to ensure overall compliance with the obligations imposed by KYC policy and the PML act.

This policy was last reviewed and approved by the Board on 6th November 2019