Anti Money Laundering Policy and KYC Norms

Effective Date: 01.11.2019

Contents

Anti Money Laundering Policy and KYC Norms

Effective Date: 01.11.2019

1. Background

The Prevention of Money Laundering Act (PMLA) 2002 came into effect from 1 July 2005 through a Gazette of India notification of even date. As per the PMLA 2002 read with Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 including any amendment thereof (PMLR 2005) (PMLA 2002 and PMLR 2005 will together referred to as PMLA), the offence of Money Laundering is defined as:

"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. "Proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to scheduled offence or the value of any such property."

Reserve Bank of India (hereinafter 'RBI'), one of the regulatory agencies entrusted with the responsibility of driving the anti-money laundering initiatives advised NBFCs to follow certain customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority. RBI revisited these guidelines from time to time keeping in view the recommendations of Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT).

RBI came up with detailed guidelines based on the above and the instructions issued on Customer Due Diligence (CDD) for Non-banking Financial Companies by the Basel Committee on Banking Supervision. RBI advised NBFCs to ensure that a proper policy framework on 'Know Your

Customer' and Anti-Money Laundering measures with the approval of the Board is formulated and put in place. Accordingly, Gramadhar has in place Board approved Anti Money Laundering Policy and KYC Norms (the Policy). Based on the experience gained over the past years, the Policy is proposed to be reviewed and improved keeping in view the Master Circular on the subject issued by RBI on 1 July 2014, the revised guidelines vide circular no RBI/2014- 15/330 DNBR (PD).CC. No. 005 /03.10.42/2014-15 dated 1 Dec 2014 and Know Your Customer (KYC) Direction, 2016 which is to be read along with the extant Directions issued by the RBI in this regard or any other applicable law in force.

2. Definition

1. **"*Beneficial Owner*" ('BO')** in relation to a customer is a person or an entity who is to be considered a beneficiary of the financial transaction entered in to with the Company by the customer. A list of persons who are to be considered as such BOs in relation to a customer is given below:

Type of Customer	Persons to be considered Beneficial Owners (BOs)
Public / Private Limited Companies	a) A natural person having, whether alone or together, or through one or more juridical person, ownership of or entitlement to more than twenty-five percent of shares or capital or profits of the company; or b) A natural person having, whether alone or together, or through one or more juridical person, right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements; or c) Where none of the above is been identified – a natural Person who holds the position of senior managing official.
Partnership Firm	a) A natural person having, whether alone or together, or through one or more juridical person, ownership of/ entitlement to more than fifteen percent of capital or profits of the partnership; or b) Where the above is not been identified – a natural person who holds the position of senior managing official
Unincorporated association of persons or body of individuals	a) A natural person having, whether alone or together, or through one or more juridical person, ownership of/ entitlement to more than fifteen percent of property or capital or profits of such association or body of individuals; or

	b) Where the above is not been identified – a natural person who holds the position of senior managing official
Trust/ Foundation	a) The Author of the trust; or b) The Trustees of the trust; or c) The Beneficiaries of the trust with fifteen percent or more interest in the trust; or d) A natural person exercising ultimate effective control over the trust through a chain of control or ownership

Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or Beneficial Owner of such companies.

2. **“Customer”** for the purpose of this Policy would have the same meaning as assigned to it under the RBI’s Guidelines on ‘Know Your Customer’ and Anti-Money Laundering Measures, as amended from time to time.
3. **“Customer Due Diligence (CDD)”** means identifying and verifying the customer and the Beneficial Owner using ‘Officially Valid Documents’ as a ‘proof of identity’ and a ‘proof of address’ in the manner provided under this Policy read along with the manner prescribed under the RBI’s Guidelines on “Know Your Customer” and Anti-Money Laundering Measures, as amended from time to time.
4. **“Central KYC Records Registry” (CKYCR)** means the Company, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.
5. **“Reporting Entity”** for the purpose of this Policy would mean the Company, Gramadhar Finserve Private Limited.
6. **“KYC Templates”** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
7. **“Suspicious transaction”** means a “transaction” as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:
   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 appears to be made in circumstances of unusual or unjustified complexity; or appears to not have economic rationale or bona-fide purpose; or gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

3. Important provisions under PMLA

The offense of money laundering is defined as “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”

Punishment for Money Laundering is laid down as “whoever commits the offense of money laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but may extend to seven years and shall also be liable to fine which may extend to five lakh rupees”.

Every banking company or financial institution and intermediary or a person carrying on designated business or profession (hereinafter “reporting enterprise”) is required to:

Maintain a record of all transactions the nature and value of which may be prescribed, whether such transaction comprise of a single transaction or series of transactions integrally connected to each other and where such series of transactions take place within a month.

Furnish information of transactions referred to in the clause above to the Director (FIU IND) within such time as may be prescribed.

Verify and maintain records of the identity of all its clients, in such a manner as may be prescribed.

Identify Beneficial Owner, if any, of such of its clients, as may be prescribed.

Maintain record of documents evidencing identity of its clients and Beneficial Owners as well as account files and business correspondence relating to its clients.

Where the Principal Officer of a banking company or financial institution or intermediary, as the case may be, has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed value so as to defeat the provisions of this section, such officer shall furnish information in respect of such transactions to the Director-FIU IND within the prescribed time.

The records referred to above shall be maintained for a period of ten years from the cessation of the transactions between the clients and the banking company of financial institution or intermediary, as the case may be. However, details furnished to Director FIU-IND, documents related to identity and Beneficial Owner of the client shall be maintained permanently.

The reporting entities shall have “Designated Director" designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules thereof. The Designated Director can be any one of the Managing Director or a whole-time Director or a person who holds the position of senior management (One level below the Board) or equivalent, duly authorized by the Board of Directors of the company.

However, in no case, the principal officer shall be nominated as the "Designated Director" for the purpose of this Policy.

The Director-FIU IND may whether on his own or on an application made by an authority, officer or person call for records referred to above and may make such inquiry or cause such inquiry to be made, as he thinks fit, with respect to obligations of the reporting entity.

If the Director-FIU IND, in the course of any inquiry, finds that a banking company, financial institution or intermediary or any of its officers has failed to comply with the provisions for maintenance of records, furnishing of information, verification of identity of customers etc., then without prejudice to any other action that may be taken under any other provisions of PMLA, Director – FIU-IND may, by an order, levy a fine on such banking company or financial institution or intermediary which shall not be less than ten thousand rupees but may extent to one lakh rupees for each failure.

4. Know Your Customer (KYC) Standards

Gramadhar KYC standards would include the following elements

4.1 Customer Acceptance Policy

Gramadhar proposes the following customer acceptance policy:

The company shall not undertake any transaction with entity that has fictitious/ benami name(s).

All the Customers would be classified under two heads viz. Low Risk and Medium/High Risk.

The Low Risk Customers would be the Individuals (other than High Net worth Individuals with NW of over Rs.100 lacs) 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 (salaried employees, people belonging to lower economic strata)

High/Medium Risk Customers would include (a) non-resident Customers, (b) high net worth individuals (NW exceeding Rs.100 lacs), (c) trusts, charities, NGOs and organizations receiving donations, (d) companies having close family shareholding or Beneficial Ownership, (e) firms with 'sleeping partners', (f) politically exposed persons (PEPs), (g) non-face to face Customers and (h) those with dubious reputation as per public information available, etc.

PEPs - prominent public figures of foreign country (Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.) would be subjected to enhanced Customer Due Diligence (CDD) and such accounts would be permitted at least at a level higher than what is otherwise permitted to approve the account. Close relative of PEP also would be treated at par with PEP

In the case of proprietorship firms, in addition to the proprietor's ID, the firm’s ID (business proof) also would be obtained at least through any of the following two documents:

Proof of the name, address and activity of the firm, namely Registration Certificate (if registered), Shops & Establishment Certificate, Sales and Income Tax Returns, CST/ VAT Certificate etc.

Any registration / licensing document issued in the name of the firm by the Central Government or State Government Authority/ Department.

The complete ITR including the acknowledgement, issued in the name of the sole proprietor wherein the firm's income is reflected, duly authenticated/acknowledged by the IT Authorities.

Utility bills namely electricity/ water/ or landline telephone bills issued in the name of the firm.

In cases, where it is not possible to furnish any two of the above documents, the Company may accept any one of above stipulated document subject to field investigation done for the proprietorship firm.

In the case of firms reconstituted and the companies that changed the name within the past two years, the CDD would be enhanced.

For all the Customers irrespective of the risk categorization, Gramadhar would undertake following customer acceptance procedure without fail:

- Internal dedupe - Checking the internal records of Gramadhar to confirm about any past dealings of the Customer with Gramadhar either as borrower, co-borrower or guarantor;
- External dedupe – Verifying with the data base maintained by at least one RBI approved credit information bureau;
- Field investigation of Customer’s residence and office. Neighborhood check;
- Trade reference check in the case of commercial lending;
- Tele verification with the Customer and underwriting;

Documentation requirements and other information to be collected in respect of different categories of Customers depending on perceived risk and keeping in mind the requirements of PMLA and guidelines issued by Reserve Bank from time to time.

The company shall not start or close a business transaction where the company is unable to apply appropriate Customer due diligence measures i.e. the company is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non-cooperation of the Customer or non-reliability of the data/information furnished to the company. It may, however, be necessary to have suitable built in safeguards to avoid harassment of the Customer.

In case of existing business relationships, if the Customers are not KYC compliant, the Company will take necessary measures to carry out necessary actions to comply with the requirements and where the Company fails to do so, it will take necessary measures to either terminate the existing relationship or carry out necessary actions to partially freeze the business relationship in accordance with the provisions of the RBI's Guidelines on "Know Your Customer" and Anti-Money Laundering Measures, as amended from time to time, have been complied with.

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., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs).

If an existing KYC compliant Customer desires to open another account, there would be no need for submission of fresh proof of identity and/or proof of address for the purpose.

The System is being enabled to capture Customer classification from Money Laundering perspective and the data capture and analysis would follow as soon as the System is enabled.

4.2 Customer Identification Procedure

Gramadhar shall ensure adherence of Customer Identification Procedure as prescribed by the Reserve Bank of India from time to time. Gramadhar would obtain the KYC documents whenever there is doubt about the authenticity/veracity or the adequacy of the previously obtained Customer identification data. If Aadhaar card is taken as KYC, Gramadhar would satisfy itself about current address by obtaining required proof. Gramadhar also have the process of allotting Unique Customer Identification Code (UCIC) for easy identification of all the relationships of any Customer with Gramadhar.

Information collected for the purpose of opening of account would be kept as confidential and would not be divulged to outsiders for cross selling or any other purpose other than for the statutory requirement of sharing the Customer account details with at least one credit information agency approved by RBI. Information sought from the Customer would be relevant to the perceived risk and would not be intrusive.

The Beneficial Owner in the case of trust, partnership and Joint stock companies would be reckoned in pursuance of this policy.

4.3 Monitoring of Transactions

Magma would continue to maintain proper record of all cash transactions of Rs.10 lakh and above and have in place centralised internal monitoring system at head office. Magma shall obtain copy of PAN of all the Customers for cash transaction of Rs 50,000 or more entered into with them. In case a Customer does not have a PAN, Form 60, duly signed by the Customer along with a valid identity proof and signature proof, should be accepted.

Magma would strive to have an understanding of the normal and reasonable activity of the Customer through personal visits and by observing the transactions and conduct of the account in order to identify transactions that fall outside the regular pattern of activity – unusual transactions.

For the simplicity of data capture, the following transactions would be considered as unusual transactions deserving special attention. Such accounts would be treated as Medium/High Risk Customers after review of the unusual transactions by the Principal Officer – PMLA.

Repeated pre termination of loan accounts of size exceeding Rs.10 lacs;

Same Customer appearing in the Cash Transaction Report (CTR) more than 3 times during a span of 6 months;

Total cash received from a customer exceeding Rs. 50 lacs in a financial year or Rs. 25 lacs in a month;

Being an NBFC, Magma is not empowered to seize any counterfeit currency like in the case of banks. However, the following incidents of counterfeit currency at the cash counters would be recorded and repeated occurrence would be reported.

Bulk counterfeit currency of more than 10 pieces at a time;

Repeated event within a week from a collection executive or Customer;

All such transactions would be reported to and reviewed by Principal Officer – PMLA who would enquire into the matter and decide whether the transaction would qualify to be termed as a suspicious transaction. When it is believed that we no longer are satisfied that we know the true identity of the account holder, STR would be filed with FIU-IND. The Principal Officer - PMLA would file the Suspicious Transaction Report (STR) with the Director, Financial Intelligence Unit-India (FIU-IND) within 7 days of identifying them. After filing STR, transactions would be allowed to be continued in the account unhindered and the Customer would not be tipped in any manner.

All CTR/STR would be filed electronically or as per the norms stipulated by FIU-IND from time to time. The STR would be filed even for attempted transactions

List of individuals and entities, approved by UN Security Council Committee and circulated by RBI would be updated and the list would be available at every office entrusted with the responsibility of customer acceptance and would be verified before opening an account. Financial Action Task Force (FATF) statements regarding countries with deficient AML/CFT would be verified and caution would be exercised with Customers who conduct business activities in these countries.

Gramadhar has a laid down Document retention policy which would be reviewed periodically to be in compliance to the requirements of PMLA. The following documents/ records would be held for a period of 10 years:

- Records with respect to the cash transactions of value of more than Rs. 10 lacs
- Records with respect to series of cash transactions integrally connected to each other of more than Rs.10 lacs within a month
- Records with respect to transactions where counterfeit currency notes have been used
- Records with respect to all suspicious transactions

- KYC documents after the business relationship ending.
  The documents/ records maintained would hold the following information

  Nature of transaction;

- Amount of the transaction;
- Date on which the transaction was conducted; and
- The parties to the transaction;
- All the units reporting the unusual transactions to Principal Officer – PMLA would be subjected to audit by Internal Audit Department.

4.4 Risk Management

The following elements of Gramadhar would manage the Risk arising out of the non- compliance to PMLA

Board would ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensure their effective implementation;

Internal audit and compliance function would evaluate and ensure adherence to the KYC policies and procedures and provide independent evaluation of Gramadhar own policies and procedures, including legal and regulatory requirements. 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 would be put up before the Audit Committee of the Board on quarterly basis;

Gramadhar would have an on-going employee training programme with different focuses for frontline staff, compliance staff and staff dealing with new Customers and educating them with respect to the objectives of the KYC Programme.

The risk categorization would be reviewed on real time basis based on the Collection feedback and enhanced due diligence measures would be applied in case of higher risk perception on a Customer.

Periodical updating of Customer identification data would be taken up once in eight years for Low/medium risk Customers and once in two years for high risk Customers. For low risk customers the updating would be only through a self-certification by the Customer in cases where there is no change in the status with respect to their identities and addresses. In case of change of address of such 'low risk' Customers, they would be merely asked to submit a certified copy of the document (proof of address) in any manner by mail/post, etc.

Fresh photographs would be obtained from minor Customers upon becoming major.

A senior management officer would be designated as the Principal Officer – PMLA and would report to senior management and the Principal Officer – PMLA would have staff to verify KYC/AML compliance. The Principal Officer – PMLA would perform the following duties

- Develop effective Anti Money Laundering programs, including training programs
- Assist business in assessing how the System can be abused
- Identify suspicious activity
- Monitor implementation of Anti Money Laundering Policy and KYC Norms
- Submit reports to statutory bodies, management and maintain liaison

5. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the KYC templates prepared for ‘individuals’ and ‘Legal Entities’ as the case may be.

6. Reporting of information with the FIU-IND

The Company will make necessary arrangements from time to time to ensure compliance with the various reporting requirements as per the RBI’s guidelines on “Know Your Customer” and Anti-Money Laundering Measures or any other applicable law in force.