Magma Fincorp Limited

Magma has in place Board approved Anti Money Laundering Policy and KYC Norms. The Policy is proposed to be reviewed keeping in view the RBI Guidelines issued from time to time.

Anti Money Laundering Policy and KYC Norms

Effective Date: 31.01.2020

Approval Date: 31.01.2020

Version No.: 9

Approved by: Board of Directors

Policy Owner: RBI Compliance Officer

Subject: **Anti-Money Laundering Policy and KYC Norms**	Original Issue Date: 18.10.2012	Effective Date: 31.01.2020
	Revision Dates: 04.02.2015, 01.08.2015, 12.05.2016, 03.11.2016, 09.11.2017, 09.05.2018, 31.01.2019, 31.01.2020	Policy Version: 9

Base Document	:	Prevention of Money Laundering Act, 2002, including amendment thereof, read with master Circular on the subject issued by RBI on 1 Jul 2014 and Know Your Customer (KYC) Direction issued by RBI as amended from time to time.
Initial Document Prepared by	:	RBI Compliance team
Functional aspects checked by	:	All vertical heads (Sales, Credit, Operation, Collections, Accounts, Information Technology, Internal Audit)
Governing Guideline/Policy	:	RBI Guidelines on KYC and AMLA
Legal aspects checked by	:	Vinod Kothari & Company, Ms. Shabnum Zaman, Mr. Anand Roy, Mr. Jitendra Maheshwari

Contents

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, Magma Fincorp Limited (‘Company’, ‘Magma’) has put in place a Board approved policy on Anti Money Laundering measures 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, as amended from time to time, (‘RBI’s Guidelines’) which is to be read along with the extant Directions issued by the RBI in this regard or any other applicable law in force. The Company shall further ensure compliance with the provisions of Prevention of Money-Laundering Act, 2002 (“Act”) and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (“Rules”), as amended from time to time, including operational instructions issued in pursuance of such amendment(s).

2. Definition

Aadhaar number", shall mean the Aadhaar number as defined in Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

Authentication", in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016**.**

"*Beneficial Owner*" ('BO') shall have the meaning as per table 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.

"Certified Copy of OVD" - Obtaining a certified copy by the Company shall mean comparing the copy of officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the Company.

"Central KYC Records Registry" (CKYCR) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer;

"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.

"Customer Due Diligence (CDD)" means identifying and verifying the customer and the Beneficial Owner using 'Officially Valid Documents' or 'Identification information as mentioned under section 15 of the RBI's Guidelines, 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.

"Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the RE as per the provisions contained in the PMLA.

"Equivalent e-document" has been defined in Section 3 as an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per Rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

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

a. Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
b. Where the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:
   i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

ii. property or Municipal tax receipt;
iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;

c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above
d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

"Offline Verification", means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the Aadhaar regulations.

"Principal Officer" means an officer nominated by the RE, responsible for furnishing information as per rule 8 of the Rules.

"Reporting Entity" for the purpose of this Policy would mean the Company, Magma Fincorp Limited.

"KYC Templates" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

"Video based Customer Identification Process (V-CIP)": a method of customer identification by an official of the RE by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer.

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".

- The Company shall:
  - 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

Magma's KYC standards would include the following elements

4.1 Customer Acceptance Policy

Magma proposes the following customer acceptance policy:

- The Company shall not undertake any transaction with entity that has fictitious/ benami name(s) or where Company is unable to apply appropriate customer due diligence (CDD) measures.

- Company shall not undertake transaction or account based relationship without following the CDD procedure and apply the same at the UCIC level. Thus, if an existing KYC compliant customer of a RE desires to open another account with the same RE, there shall be no need for a fresh CDD exercise.

- Company shall follow CDD process for all joint holders account also;

- Any information other than mandatory information required for obtaining account based relationship with the customer, maybe obtained by the Company, after obtaining explicit consent of the customer for the same.

- The Company shall ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by the RBI.

- Where an equivalent e-document is obtained from the customer, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 ('IT Act')

- Politically Exposed Persons (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 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.

4.2 Customer Due Diligence

- In case of an Individual customer, the Company shall obtain the following:

  a. The proof of possession of Aadhaar number where offline verification can be carried out; or

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

  c. PAN or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

  d. Such other documents including in respect of the nature of business and financial status of the Customer, or the equivalent e-documents thereof as may be required by the Company:

  Provided that where the customer has submitted:

  i) proof of possession of Aadhaar as above where offline verification can be carried out, the Company shall carry out offline verification;

  ii) an equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 and take a live photo as specified under **Annexure I – Digital KYC**.

  iii) any OVD or proof of possession of Aadhaar number as above, where offline verification cannot be carried out, the Company shall carry out verification through digital KYC as specified under **Annexure I – Digital KYC**.

  Offline verification of Aadhaar can be accomplished by two means:

  Via the QR code on Aadhaar card & E-Aadhaar PDF

  By downloading Offline Aadhaar file (a password protected ZIP file containing an XML file) from UIDAI's website which shall be verified through OTP sent to the mobile number of the customer.

  Detailed process for carrying out offline verification of Aadhaar is listed at **Annexure II**.

- In the case customer is a proprietorship firms, CDD of proprietor's shall be carried in the same manner as provided above. In addition to the above any of the following two

documents or equivalent e-documents as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

- Proof of the name, address and activity of the firm, namely Registration Certificate (if registered), Import & Export issued to the proprietary concern by the office of DGFT, Shops & Establishment Certificate, Sales and Income Tax Returns, CST/ VAT/GST Certificate (provisional/final) 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.
- In case customer is a company, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
  - Certificate of incorporation;
  - Memorandum and Articles of Association;
  - PAN of the company;
  - A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf;
  - Documents, of beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company’s behalf in the manner as mentioned in the policy;
- In case customer is a partnership firm, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained;
  - Registration certificate as proof of registration of the firm;
  - Partnership deed

- PAN of the partnership firm
- Documents, of beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf in the manner as mentioned in the policy;

- In case customer is a Trust, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
  - Registration certificate
  - Trust deed
  - Permanent Account Number or Form No.60 of the trust
  - Documents, of beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf in the manner as mentioned in the policy;

- In case customer is a unincorporated association or a body of individuals, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
  - Resolution of the managing body of such association or body of individuals;
  - PAN or Form No. 60 of the unincorporated association or a body of individuals
  - Power of attorney granted to transact on its behalf
  - Documents, of beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf in the manner as mentioned in the policy;
  - Certificate 80G and/or 12A, if any;

- For all the customers irrespective of the risk categorization, Magma would undertake following customer acceptance procedure without fail:
  - Internal dedupe - Checking the internal records of Magma to confirm about any past dealings of the customer with Magma 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. Neighbourhood 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 CDD 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.

- 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).

Proof of possession of Aadhaar number (with specific consent of the customer) and copy of the PAN Card (Form 60 in case the Customer does not have a PAN) shall be obtained from all new individual customers (from each party to the Agreement) and authorized Signatory of Legal Entity while establishing an account based relationship. In case Aadhaar number has not been assigned to an individual, proof of application of enrolment for Aadhaar shall be obtained wherein the enrolment is not older than 6 months and certified copy of an OVD containing details of identity and address and one recent photograph shall be obtained.

The documents to be obtained from Individual not eligible to be enrolled for an Aadhar, or a person who is not a resident shall be PAN or Form 60 (in case the Customer does not have a PAN) , as amended from time to time, one recent photograph and certified copy of OVD containing details of identity and address.

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 should be in place to capture Customer classification from the Money Laundering perspective including flagging of negative profile customers, terrorist organizations as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) etc.

4.3 Customer Identification Procedure

Magma shall ensure adherence of Customer Identification Procedure as prescribed by the Reserve Bank of India from time to time. Magma would obtain the KYC documents whenever there is doubt about the authenticity/veracity or the adequacy of the

previously obtained Customer identification data. Magma would satisfy itself about current address by obtaining required proof. Magma also have the process of allotting Unique Customer Identification Code (UCIC), after carrying out the CDD process, for easy identification of all the relationships of any Customer with Magma.

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.

Company may carry out Video based Customer Identification Process (V-CIP) as a consent based alternate method of establishing the customer's identity, for customer onboarding. V-CIP shall be carried out in the manner provided in the **Annexure I** of the policy.

4.4 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 Aadhar Card and 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.

For cash deposits of Rs 50,000 or more made by any Third Party on behalf of the customer, an Authorization letter and self-attested PAN of the customer (in case the Customer does not have a PAN, Form 60 in lieu thereof) along with an I.D proof of the person depositing the cash shall be obtained.

During sale of Repossessed assets, copy of the PAN Card or Form 60 (in case the Customer does not have a PAN), shall be obtained from the buyer of the vehicle in case the consideration amount is in excess of Rs 50,000 and is being paid in cash.

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.

Magma 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.

4.5 Risk Management

The following elements of Magma 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;
- All the Customers would be classified under three heads viz. Low Risk, Medium Risk and High Risk. Risk parameters for risk categorization of customers is appended as Annexe in this policy.
- Internal audit and compliance function would evaluate and ensure adherence to the KYC policies and procedures and provide independent evaluation of Magma's 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;

Magma 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.

A system of periodic review of risk categorization of accounts, at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

Periodical updating of Customer identification data would be taken up once in ten years for Low, once in eight years for medium risk Customers and once in two years for high risk Customers as per the following procedure:

a. Company shall carry out:
   i. CDD at the time of periodic updation. However, 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.

   ii. In case of Legal entities, Company shall review the documents sought at the time of opening of account and obtain fresh certified copies.

b. The Company shall ensure to provide acknowledgment with date of having performed KYC updation.

In case of existing customers, RE shall obtain the Permanent Account Number or equivalent e-document thereof or Form No.60, by such date as may be notified by the Central Government, failing which RE will not take additional exposure on such customer, till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer.

A senior management officer would be designated as the Principal Officer – PMLA and would report to senior management. 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
- Ensure verification of KYC/AML compliance by the front desk staff/officers

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, RBI KYC Master Directions issued from time to time, as required by the KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. Magma shall at the time of receipt of the Aadhaar number, shall carry out, with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) or Yes/No authentication.

Yes/No Authentication if carried out for existing A/c then E-KYC Authentication (Biometric or OTP based) has to be done within 6 months of yes/No authentication. Yes/No authentication cannot be done for a new on boarding customer.

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.

7. Change Control Sheet

Version No.	Change request by	Memorandum of Change	Approval date
2.0	Mr. D . Krishnaraj	To align with revised RBI Guidelines	04.02.2015
3.0	Mr. Kailash Baheti	To align with revised RBI Guidelines	01.08.2015
4.0	Mr. Gauri Shankar Agarwal (GS2) and Mr. Atul Tibrewal	To align with revised RBI Guidelines	12.05.2016
5.0	Mr. Atul Tibrewal	To comply with the requirement of RBI	03.11.2016
6.0	RBI Compliance Officer	To comply with the requirement of RBI	09.11.2017
7.0	RBI Compliance Officer	To comply with the requirement of RBI	09.05.2018
8.0	Internal Auditor & Risk Team	To comply with the requirement of Internal Audit team	31.01.2019
9.0	RBI Compliance	To include amendment vide notification dated 09.01.2020.	31.01.2020

****

Parameters for Risk Categorization of Customers				
Category	**Condition**	**Risk Category for ABF**	**Risk Category for SME, SME-C & Mortgage**	**Risk Category for Auto Lease**
Net worth	Less than 100 lacs	Low		
	100 lacs to 200 lacs	Medium		
	More than 200 lacs	High risk		
Nationality	Non -Resident Indian (all non-resident Indian cases)	High risk		
Private ltd / Ltd companies and unlisted companies.	For cases other than Individual and Public companies, if shareholding for any owner >25%	Medium		
Other than companies (Firms)	For cases other than Individual and Public companies, if shareholding for any owner >15 %	Medium		
For constitution like Trust and charities	For all cases where constitution is Trust ,Charitable organization or NGO	Medium		
Credit flag *	For all cases wherever tagged in the LOV as YES	High risk		
Auto Lease - Rating Grade with debt	Companies rated with investment grade i.e. BBB rating or above from the rating agencies accredited with SEBI.			Low
	Unrated companies without debt			Medium
	Rating below BBB or Unrated companies with debt			High
SME & Mortgage - Loan Sanction amount	Loan Sanction <=50 Lacs		Low	
	Loan sanction >50 lacs <=100 lacs		Medium	
	Lan Sanction >100 Lacs		High	
SME – C	Loan sanction <=10 crore		Low	
	Loan sanction > 10 crore and <=25 crore		Medium	
	Loan sanction > 25 crore		High	
Buy Out Portfolio	If risk parameters of the seller is same as the risk parameters of the Company (as above) or underlying information for (re)alignment of risk (re)categorization is available, risk categorization of portfolio shall be			

	same as of the Company. If risk parameters of the seller is different from the risk parameters of the Company and the underlying information for (re)alignment of risk (re)categorization is not available, the risk categorization of the buyout portfolio of the seller shall be taken as risk categorization for the Company.

Note: For all the party codes ,the rule for medium /high risk will supersede other rules. Example: If NW less than 100 but nationality is Non-resident, system will tag the case as High risk Profile.

*** Credit Flag**	**List of Values (LOV)**	**Status**
Credit High Risk at Credit Approval Stage	Closed Family shareholding	Y/N
	Sleeping Partner	Y/N
	Poitically exposed person	Y/N
	Non Face to Face Customer	Y/N
	Dubious reputation as per public information	Y/N
	Firm Reconstitute	Y/N
	Company name changed	Y/N

Annexure I

Digital KYC Process

A. The Company shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the Company.

B. The access of the Application shall be controlled by the Company and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by Company to its authorized officials. C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the RE or vice-versa. The original OVD shall be in possession of the customer.

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

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

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

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

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

Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

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

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

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

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

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

Video-Customer Identification Process

The Company may undertake live V-CIP, carried out by an official of the Company, for establishment of an account based relationship with an individual customer, after obtaining his informed consent and shall adhere to the following stipulations:

i. The Company shall authorise its officials to carry out CDD who shall be referred to as Authorised officer/Authorised official. The Authorised official shall record video as well as capture photograph of the customer present for identification and obtain the identification information through Offline Verification of Aadhaar for identification.

ii. The Company shall capture a clear image of PAN card displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority.

iii. Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India

iv. The Authorised official of the Company shall ensure that photograph of the customer in the Aadhaar/PAN details matches with the customer undertaking the V-CIP and the identification details in Aadhaar/PAN shall match with the details provided by the customer.

v. The Authorised official shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

vi. In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.

vii. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process.

viii. Company shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audio-visual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt.

ix. To ensure security, robustness and end to end encryption, the Company shall carry out software and security audit and validation of the V-CIP application before rolling it out.

x. The audio-visual interaction shall be triggered from the domain of the Company itself, and not from third party service provider, if any. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

xi. Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.

xii. The Company shall ensure to redact or blackout the Aadhaar number.

Annexure II

Process of Offline Verification

UIDAI has launched Aadhaar Paperless Offline e-KYC Verification to allow Aadhaar number holders to voluntarily use it for establishing their identity in various applications in paperless and electronic fashion, while still maintaining privacy, security and inclusion.

UIDAI provides a mechanism to verify identity of an Aadhaar number holder through an online electronic KYC service. The e-KYC service provides an authenticated instant verification of identity and significantly lowers the cost of paper based verification and KYC. However, this method of online e-KYC is not available to all agencies and may not be suitable due to some of the following reasons;

- Online e-KYC requires reliable connectivity
- Agency needs to have technical infrastructure to call online e-KYC service and deploy devices (as necessary)
- The resident may need to provide biometrics for the online e-KYC
- UIDAI maintains a record of the KYC request for audit purposes

Advantages of Aadhaar Paperless Offline e-KYC Privacy:

- KYC data may be shared by the Aadhaar number holder directly without the knowledge of UIDAI.
- Aadhaar number of the resident is not revealed, instead only a reference ID is shared.
- No core biometrics (fingerprints or iris) required for such verification
- Aadhaar number holder gets a choice of the data (among the demographics data and photo) to be shared.

Security:

- Aadhaar KYC data downloadable by Aadhaar number holder is digitally signed by UIDAI to verify authenticity and detect any tampering.
- Agency can validate the data through their own OTP/Face Authentication.
- KYC data is encrypted with the phrase provided by Aadhaar number holder allowing residents control of their data.

Inclusion:

- Aadhaar Paperless Offline e-KYC is voluntary and Aadhaar number holder driven.
- Any agency working with people can use it with consent of the Aadhaar number holder allowing wide usage.

Aadhaar Paperless Offline e-KYC eliminates the need for the resident to provide photo copy of Aadhaar letter and instead resident can download the KYC XML and provide the same to agencies wanted to have his/her KYC. The agency can verify the KYC details shared by the resident in a manner explained in below sections. The KYC details is in machine readable XML which is digitally signed by UIDAI allowing agency to verify its authenticity and detect any tampering. The agency can also authenticate the user through their own OTP/Face authentication mechanisms.

How to obtain Aadhaar Paperless Offline e-KYC Data

Aadhaar number holders can obtain Aadhaar Paperless Offline e-KYC data through the following channels:

- Download Aadhaar Paperless Offline e-KYC from resident portal (https://resident.uidai.gov.in)
- In future, obtain Aadhaar Paperless Offline e-KYC will also be available via:
- mAadhaar mobile application on a registered phone number
- Inbound SMS using registered phone number
- Aadhaar Kendra using Biometric Authentication