Introduction (KNOW YOUR CUSTOMER (KYC) AND ANTI-MONEY LAUNDERING (AML))

The Reserve Bank of India has issued directions on Know Your Customer (KYC) norms and Anti-Money Laundering (AML) standards and has advised all NBFCs to ensure that a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the board of directors of the Regulated Entities. Citra Financials Private Limited ("the Company" or "Citra"), being a Regulated Entity, has to comply with the aforementioned directions on KYC and AML.

In view of the same, the Board of Directors of the Company ("Board") in compliance with the Master Direction - Know Your Customer (KYC) Direction, 2016 issued by Reserve Bank of India vide its notification bearing no. DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016, with any amendment/re-enactment thereof issued from time to time ("RBI Master Direction") and the Prevention of Money Laundering Act, 2002 ("Act") read with the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 ("Rules") with any further amendments/ re-enactments thereof issued from time to time, has adopted a policy on 'Know Your Customer' (KYC) and 'Anti-Money Laundering (AML) Measures' ("KYC-AML Policy").

The objective of these guidelines for the Company is to know/understand its customers and their financial dealings and help the Company to manage its risks prudently. It is also to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering/anti-national activities.

APPLICABILITY

It may be noted that KYC – AML Policy as stated in this document shall prevail over anything else contained in any other document/process/circular/letter/instruction of the Company in this regard (KYC-AML). This policy shall be applicable to all verticals/products of the Company whether existing or to be rolled out in future.

DEFINITIONS

- ✓ “Aadhaar number” shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 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.

- ✓ “Customer” means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting

- ✓ “Act” and “Rules” means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

- ✓ “Customer Due Diligence (CDD)” means identifying and verifying the customer and the beneficial owner

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

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

- ✓ “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 authorized officer of the RE as per the provisions contained in the Act.

- ✓ “Digital Signature” shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

- ✓ “Equivalent e-document” means 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.

- ✓ “Know Your Client (KYC) Identifier” means the unique number or code assigned to a customer by the Central KYC Records Registry.

- ✓ “Officially Valid Document” (OVD) means the passport, the driving license, proof of possession of Aadhaar card, 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, where the customer submits his proof of possession of Aadhaar as an OVD, he may submit it in such form as issued by the Unique Identification Authority of India.

- ✓ “Digital Platform” means mobile app and/or web-based platform through which the Company provides personal loans and advances to its Customers.

- ✓ “Principal Officer” means an officer nominated by the Company, responsible for furnishing information as per rule 8 of the Rules

- ✓ “Transaction” means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

    - ✓ opening of an account.

    - ✓ deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means.

    - ✓ the use of a safety deposit box or any other form of safe deposit.

    - ✓ entering into any fiduciary relationship.

    - ✓ any payment made or received, in whole or in part, for any contractual or other legal obligation.

    - ✓ establishing or creating a legal person or legal arrangement.

- ✓ “Video based Customer Identification Process (V-CIP)”: a method of customer identification by an official of the Company 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. Such a process shall be treated as a face-to-face process for the purpose of this KYC Policy.

ELEMENTS OF THIS POLICY

The Company’s KYC-AML policy has the following four key elements:

- ✓ Customer Acceptance Policy;

- ✓ Customer Identification Procedure

- ✓ Monitoring of Transactions and

- ✓ Risk management

Customer Acceptance Policy

The Customer Acceptance Policy of the Company is aimed at ensuring that explicit guidelines are in place on the following aspects of customer relationship with the Company:

- ✓ No loan account will be opened and / or money will be disbursed in a name which is anonymous or fictitious/ benami name or appears to be borrowed.
- ✓ Accept customers only after verifying their identity, as per CDD, and if the Company is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer then no account will be opened.
- ✓ No Transaction or account-based relationship is undertaken without following the CDD procedure.
- ✓ The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, as specified.
- ✓ Optional/ additional information is obtained with the explicit consent of the customer after the account is opened.
- ✓ Circumstances, in which a customer is permitted to act on behalf of another person /entity, shall be clearly spelt out in conformity with the established law and practices, as there could be occasions when an account is operated by a mandate holder or where an account may be opened by intermediary in a fiduciary capacity.
- ✓ Suitable system shall be put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.

Subject to the above-mentioned norms and caution, at the same time all the employees of Company will also ensure that the above norms and safeguards do not result in any kind of harassment or inconvenience to bona fide and genuine customers who should not feel discouraged while dealing with the Company.

It is important to bear in mind that the adoption of Customer Acceptance Policy and its implementation should not become too restrictive and must not result in denial of the company’s services to the general public, especially to those, who are financially or socially disadvantaged.

Customer Identification Procedure

Customer identification means identifying and undertaking Customer Due Diligence (CDD) of the Customer and verifying his / her identity by using reliable, independent source documents, data or information. The Company needs to obtain enough information necessary to establish, to their satisfaction and as required by applicable law, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of the relationship. The process of Customer Due Diligence ("CDD") is mentioned in Annexure-1 of the policy.

Being satisfied means that the Company should be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer as set by the Company, in compliance with the extant guidelines in place. For customers that are natural persons, the Company shall obtain enough identification data to verify the identity of the customer, his/ her address/ location, and also his/ her recent photograph.

An indicative list of the nature and type of documents/information that shall be relied upon for customer identification is given in the KYC Documentation Policy annexed as Annexure-I

Customer Identification Procedure to be carried out at different stages as under:

- ✓ Commencement of an account-based relationship with the customer.
- ✓ When the Company has a doubt about the authenticity or adequacy of the customer identification data obtained by the Company. Customer identification means identifying the customer and verifying his/ her/ its identity by using reliable, independent source documents, data or information.
- ✓ Carrying out a financial transaction.

During the loan application process online, the Company shall not ask the customer to furnish additional proofs, if proofs submitted by the customer for KYC contain both proof of identity and proof of address as per Annexure-1. Further, the customer shall not be required to furnish separate proof of address for permanent and current addresses, if these are different. The Company shall obtain a declaration from the customer about her/ his local address on which all correspondence will be made by the Company, in the event the proof of address furnished by the customer is the address where the customer is currently residing. However, in the

physical KYC stage where authorized representatives of the Company visit Customers, Customers need to provide proof of address for current address as well.

The Company shall allot Unique Customer Identification Code to all their customers while entering into any new relationship with Customer.

Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. The officials have to effectively control and reduce the risk by having 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 each account. Officials should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

The Company may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the officials. Very high account turnover inconsistent with the means of the customer may indicate that funds are being 'washed' through/into the account. High-risk accounts have to be subjected to intensified monitoring. The Company should put in place a system of periodical review of risk categorization of accounts and apply enhanced due diligence measures wherever required.

Risk Management

For proper risk assessment of business relationship with customers, the Company profiles Customers basis on the risk perceived and it is totally system driven risk assessment model which takes in various inputs about customers from multiple non-intrusive consent based

sources & then arrives at creating risk profile which will be broadly classified as Low risk, Medium Risk and High Risk.

All the customers under different product categories are categorized into low, medium and high risk based on their profile. The Company while appraising the transaction and rendering his approval prepares the profile of the customer based on risk categorization. Based on the credit appraisal, customer's background, nature and location of activity, country of origin, sources of funds, client profile, repayment history etc. System driven risk profiling shall be done from time to time.

APPOINTMENT OF PRINCIPAL OFFICER

Company shall designate an officer nominated by the Company as 'Principal Officer' (PO) who shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the Act. PO shall maintain close liaison with enforcement agencies, NBFCs and any other institution which are involved in the fight against money laundering and CFT. The name, designation & address of the PO shall be communicated to FIU-IND and/or the department concerned of the RBI.

REPORTING TO FINANCIAL INTELLIGENCE UNIT-INDIA

As required in Section 12 of the Act the company has to report information of transaction referred to in clause (a) of sub-section (1) of section 12 read with Rule 3 of the Rules relating to cash and suspicious transactions etc. to the Director, Financial Intelligence Unit- India (FIU-IND). The proviso to the said section also provides that where the principal officer 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 of FIU-IND within the prescribed time.

The information has to be furnished at the following address by the Principal Officer:

Director, FIU-IND,

Financial Intelligence Unit-India,

6th Floor, Hotel Samrat, Chanakyapuri,

New Delhi-110021.

A copy of information furnished shall be retained by the Principal Officer for the purposes of official record.

The information in respect of the transactions referred to in clause(A), (B) and (BA) of sub-rule (1) of rule 3 of the PML Rules is to be submitted to the Director every month by the 15th day of the succeeding month.

The information in respect of the transactions referred to in clause(D) of sub-rule (1) of rule 3 of the Rules is to be furnished promptly to the Director in writing, or by fax or by electronic mail not later than seven working days from the date of occurrence of such transaction.

Provided the company and its employees maintain strict confidentiality of the fact of furnishing/ reporting details of suspicious transactions.

It has to be noted that in terms of Rule 8, while furnishing information to the Director FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a misrepresented transaction beyond the time limit as specified in this rule shall constitute a separate violation. As advised by the FIU-IND, New Delhi the Company need not submit NIL" reports in case there are no Cash/Suspicious Transactions, during a particular period.

The required information is to be furnished by the Company directly to the FIU-IND, through the Principal Officer designated by the Company under the Prevention of Money Laundering Act, 2002.

APPOINTMENT OF DESIGNATED DIRECTOR

The Board of Directors shall nominate a “Designated Director” to ensure compliance with the obligations prescribed by the Act and the Rules there under. The “Designated Director” can be a person who holds the position of senior management or equivalent. However, it shall be ensured that the Principal Officer is not nominated as the “Designated Director.” The name, designation and address of the Designated Director shall be communicated to the FIU-IND.

MAINTENANCE AND PRESERVATION OF RECORDS

Section 12 of PMLA requires to maintain records as under:

- ✓ Records of all transactions referred to in clause (a) of Sub-section (1) of section 12 read with Rule 3 of the Rules is required to be maintained for a period of five years from the date of transaction between a client and the Company.
- ✓ Records of the identity & address of all clients of the Company is required to be maintained for a period of five years after the business relationship between a customer and the company entity has ended or the account has been closed, whichever is later.
- ✓ Other records not related to identity of clients or records of transaction are to be preserved for at least for five years from the date of the record.
- ✓ For destruction of records, each department shall maintain a register under the custody of the Senior Management officer of the department concerned for maintaining records of destruction and name of the approving officers for such destruction.

The Company shall take appropriate steps to evolve a system for proper maintenance and preservation of information in a manner (in hard and soft copies) that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. The Company must maintain records of the identity of clients, and records in respect of transactions with its client referred to in rule 3 in hard or soft format.

CENTRAL KYC RECORDS REGISTRY (CKYCR) - AND REPORTING REQUIREMENTS UNDER FOREIGN ACCOUNT TAX COMPLIANCE ACT (FATCA)/ COMMON REPORTING STANDARDS (CRS)

As directed by RBI vide their circular no. RBI/2015-16/251:DBR.AML.BC.No.60 /14.01.001/2015-16 dated November 26, 2015, compliance with the Government notification

dated July 7, 2015 (amending the Prevention of Money Laundering (Maintenance of Records) Rules, 2005) needs to be ensured.

The company will upload the Know Your Customer (KYC) data with CERSAI in respect of new individual accounts (opened w.e.f Nov 01, 2016). KYC information will be captured for sharing with the Central KYC Record Registry in the manner mentioned in the “Prevention of Money-Laundering (Maintenance of Records) Rules, 2005” (and amendments thereto).

In compliance with RBI directive, the Company shall keep the KYC data ready in digital format in the templates advised by RBI of all our existing clients. The Loan Application forms of Retail clients may be revised, if required, to capture the data of clients in RBI prescribed template in future.

The Company shall also take all steps to comply with the FATCA and CRS reporting requirements, as advised by RBI and Government of India from time to time.

MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

- ✓ The Company shall carry out ‘Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment’ exercise, on an annual basis, to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk as per RBI’s guidelines.
- ✓ The risk assessment should be properly documented.
- ✓ The outcome of the exercise shall be put up to the Board of Directors to which power in this regard has been delegated, and should be available to competent authorities and self regulating bodies, if required.
- ✓ The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard.
- ✓ The Company shall monitor the implementation of the controls and enhance them if necessary.

RELIANCE ON THIRD-PARTY DUE DILIGENCE

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-

- ✓ The Company obtains records or information of such customer due diligence carried out by the third party within 7 days from the third party or from Central KYC Records Registry.
- ✓ 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.
- ✓ The Company is satisfied that such a third party is supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the applicable requirements.
- ✓ The third party is not based in a country or jurisdiction assessed as high risk.
- ✓ The Company is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

Customer Due Diligence (CDD) Procedure

For undertaking CDD, the Company shall obtain the following from an individual establishing an account-based relationship:

(A)	Proof of Identity	Scan / Image of the following document to be uploaded on Digital Platform of the Company: 1. PAN card or the equivalent e-document thereof.

(B)	Proof of Address	Scan / Image of any one of the following documents to be uploaded on Digital Platform of the Company: 1. Passport or the equivalent e-document thereof 2. Voter Identity Card or the equivalent e-document thereof. 3. Masked UIDAI card (Aadhaar) or the equivalent e-document thereof containing details of his identity and address. During the physical face to face KYC for the customers whose cumulative loan amount exceeds INR 60,000/- in a FY, if address mentioned on either of the above documents does not match with current resident address, the Customer need to mandatorily provide Current resident address proof (Rent agreement, Utility Bill (Electricity, telephone, Post-paid mobile phone, piped gas bill, water bill), Municipal tax receipt.
(C)	Real time selfie	Customers while applying for the loan need to capture one real-time selfie which will be facilitated by the Company itself through its tech-based mobile application

Note: If the aggregate of borrowal amount of the single borrower, in one or more tranches, is exceeded rupees sixty thousand in a financial year, then the Company shall carry the CDD by using physical mode or Video based Customer Identification Process (V-CIP), as per procedure mentioned in Annexure-1.

- ✓ The mandatory information to be sought for KYC purpose while opening an account and during the periodic updates as specified, should be obtained.
- ✓ 'Optional'/additional information is obtained with the explicit consent of the customer after the account is opened.
- ✓ Complying to Know Your Customer (KYC) Directions 2016, Chapter VI, paragraph 24, the Company does not ask for KYC documents again and only asks customers to upload selfie in some case basis risk assessment model.
- ✓ Accounts may be opened using OTP based e-KYC in non-face to face mode, and are also accepted subject to certain conditions.

- ✓ There must be a specific consent from the Customer for authentication through OTP.

- ✓ As regards to borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned in a year shall not exceed rupees sixty thousand in a financial year.

- ✓ A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC either with the Company or with any other financial institution.

The Company may undertake a live Video based Customer Identification Process (V-CIP), to be 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.

- ✓ The official of the Company performing the V-CIP shall record video as well as capture photographs of the customer present for identification and obtain the identification information Offline Verification of Aadhaar for identification. Further, services of Business Correspondents (BCs) may be used by the Company for aiding the V-CIP.

- ✓ The Company shall capture a clear image of the PAN card to be 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.

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

- ✓ The official of the Company shall ensure that the 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.

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

- ✓ 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.

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

- ✓ The 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. Company shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

- ✓ 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.

- ✓ The audiovisual 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.

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

- ✓ Companies are encouraged to take assistance from the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer. However, the responsibility of customer identification shall rest with the Company.

- ✓ The Company shall ensure to redact or blackout the Aadhaar number in terms of Section 16.

- ✓ BCs can facilitate the process only at the customer end and as already stated above, the official at the other end of V-CIP interaction should necessarily be a Company official. The Company shall maintain the details of the BC assisting the customer, where services of BCs are utilized. The ultimate responsibility for customer due diligence will be with the Company.

- ✓ While uploading the information to CKYCR the company must mention that such accounts have been opened through OTP based e-KYC and pending Customer Due Diligence. Once the due diligence is completed the status needs to be updated in the CKYCR portal.

Further the Company may accept e-Aadhaar downloaded from UIDAI website as an officially valid document subject to the following:

- ✓ If the prospective customer knows only his / her Aadhaar number, the company may print the prospective customer's e-Aadhaar letter in the Company’s branch/office directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in the circular.

- ✓ BLF the prospective customer carries a copy of the e-Aadhaar downloaded elsewhere, the company print the prospective customer's e-Aadhaar letter in the Company’s branch/office directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in the circular or confirm identity and address of the resident through simple authentication service of UIDAI.

Rule 9 of the Prevention of Money-Laundering (Maintenance of Records of the Nature and Value of Transactions, The Procedure and Manner of Maintaining and Time for Furnishing information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 under the Act (hereinafter referred to as PML Rules), requires the Company to:

- ✓ At the time of commencement of an account–based relationship, identify its clients, verify their identity and obtain information on the purpose and intended nature of the business relationship.
- ✓ in all other cases, verify identity while carrying out:
    - ✓ transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or
    - ✓ Any international money transfer operations.