Document Control

Item	Description
Document Title	Know Your Customer (KYC) & Anti–Money Laundering (AML/CFT) Policy
Document Owner	Shilpa Kale, Manager, Policy and Risk

Preamble:

The Reserve Bank of India (RBI) has issued guidelines on 'Know Your Customer' (KYC) Guidelines - Anti Money Laundering Standards for Non-Banking Finance Companies (NBFCs) in the context of the recommendations made by the Financial Action Task Force (FATF) and Anti Money Laundering (AML) standards and Combating Financing of Terrorism (CFT) policies. RBI has advised all regulated entities to ensure that a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Board.

"Unnatti Finserv Limited is a Non-Banking Financial Company (NBFC) and a Regulated Entity as defined under the applicable directions issued by the Reserve Bank of India (RBI). Accordingly, in compliance with the guidelines and directions issued by the RBI from time to time, the Company has adopted this KYC & AML Policy, duly approved by its Board of Directors. The provisions of this Policy shall be read in conjunction with and shall be deemed to be amended, modified, or updated in accordance with any changes, amendments, or directions issued by the RBI from time to time.
"Definitions:

"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.

Beneficial Owner (BO) Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercise control through other means.

Explanation- For the purpose of this clause

i) "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company.
ii) "Control" shall include the 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.

"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 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.

"Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include the Managing Director or a whole-time Director, duly authorized by the Board of Directors.

Officially Valid Document" (OVD) 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

"Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

"Principal Officer" means an officer nominated by the Company, responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

"Reporting Entity" for the purpose of this Policy would mean the Company, Unnatti Finserv Limited.

"Senior management" for the purpose of KYC compliance, the Managing Director/ Executive Director, Chief Executive Officer, Chief Risk Officer, Chief Compliance Officer and Chief Operating Officer are constituted as "Senior Management".

"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.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism

Objectives:

The objective of KYC & AML Policy is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures shall also enable the Company to know and understand its Customers and its financial dealings better which in turn will help it to manage its risks prudently. Thus, the said policy has been framed by the Company for the following purposes:

(i) put in place an effective system and procedure for customer identification and verifying his/ her identity and residential address based on the risk factor associated with each customer;

(ii) have in place a system of assessing and monitoring the risk factors associated with each customer;

(iii) put in place a system of checks and balances to ensure formulation and effective implementation of procedures to help control and mitigate the risk of occurrence of financial frauds, swiftly identify probable transactions of money laundering and related suspicious activities and safeguarding the Company from being unwittingly used as a conduit for transfer or deposit of funds derived from criminal activity or for financing of terrorism, irrespective of whether such money can be traced to a specific act of terrorism or not;

Customer Acceptance Policy (CAP)

UFPL has formulated a robust CAP which aims to verify the identity and address of customer by using reliable, independent source documents, data or information. It will, however, be ensured that CAP does not lead to any customer harassment or leads to denial of financial service to customers. The guidelines in respect of the customer relationship are as follows:

a) No loan account will be opened, and / or money will be disbursed in a name which is anonymous or fictitious or appears to be a name borrowed only for opening the loan account i.e., Benami Account. The Company shall insist on sufficient proof about the identity of the customer to ensure his physical and legal existence at the time of accepting the application form from any customer
b) Accept customers only after verifying their identity, as laid down in Customer Identification Procedures.
c) Documentation requirements and other information to be collected, as per PMLA and RBI guidelines/instructions, to be complied with
d) Identity of a new customer to be checked so as to ensure that it does not match with any person with known criminal background
e) Given the low-ticket size of our loans and type of clients, which includes low-income household, all our customers are considered to be of "low risk"
f) The Company will not give a loan to any applicant and shall close any existing loan where UFPL is unable to apply appropriate customer due diligence measures i.e., where the Company is unable to verify the identity and/or obtain documents required as per the extant policies to the non-cooperation of the applicant/customer or non-reliability of the data/information furnished by such applicant/customer. The decision to close any existing loan account due to failure to meet CAP shall be taken by Principal Officer
g) 'Optional'/additional information, will be obtained with the explicit consent of the customer.
h) The Company shall apply the CDD procedure at the Unique Customer Identification Code (UCIC) level. Thus, if an existing KYC compliant customer of the Company desires to open another account, there shall be no need for a fresh CDD exercise
i) The Company shall not open any account or give / sanction any loan or close an existing

account where the Company is unable to apply appropriate due diligence measures arising due to any of the following circumstances:

- The Company is unable to verify the identity of the customer
- The customer without any valid or convincing reasons refuses to provide documents to the Company
- Information furnished by the customer does not originate from the reliable sources or appears to be doubtful due to lack of supporting evidence.
- Identity of the customer, directly or indirectly matches with any individual terrorist or prohibited / unlawful organizations, whether existing within the country or internationally, or if the customer or beneficiary is found, even remotely, to be associated with or affiliated to any illegal, prohibited or unlawful or terrorist organization as notified from time to time either by Govt. of India, State Govt. or any other national or international body / organization.

j) The Company may rely on third party verification subject to the conditions prescribed by Reserve Bank of India (RBI) in this regard.

k) The information collected from the customer shall be kept confidential.

l) Subject to the above-mentioned norms and caution, at the same time the 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.

Risk Level Categorization

The Company shall categorize its customers based on the risk perceived by the Company. The levels of categorization would be Low Risk, Medium Risk and High Risk. Risk categorization shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location etc.

However the Company can do the risk categorization of its customers based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in. The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

Customer Identification Procedure

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. The Company needs to obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship. Being satisfied means that the Company must be able to satisfy the competent authorities that due diligence was observed in

compliance with the extant guidelines in place.

The Company will perform appropriate, specific and where necessary, Enhanced Due Diligence on its customers that is reasonably designed to know and verify the true identity of its customers and to detect and report instances of criminal activity, including money laundering or terrorist financing.

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

- While establishing an account-based relationship (or)
- Carrying out a financial transaction (or)
- Where the Company has a doubt about the authenticity/veracity (or)
- Inadequacy of the previously obtained customer identification data if any.
- When the Company feels it is necessary to obtain additional information from the existing customers based on the conduct or behavior of the account.

For undertaking CDD, the list of documents that can be accepted as proof of identity and address from various customers across various products offered by the Company is given as Annexure I to this policy.

Customer Due Diligence Procedures for all customers:

The Company shall take reasonable measures to ascertain and verify the true identity of all customers. The Company shall ensure that relevant documents as listed in Annexure I are obtained from prospective individual customers in order to carry out the necessary due diligence for establishing their identity.

If an existing KYC compliant customer desires to open another loan account, there is no need for submission of fresh proof of identity and/or proof of address for the purpose. However, if there is a change in the residential address of the customer, a self-declaration and new residential address proofs are taken before opening of the new account.

Risk Management

The Company has put in place appropriate procedures to ensure effective implementation of KYC guidelines. The implementation procedure covers proper management oversight, systems and controls, segregation of duties, training and other related matters. The Field staffs of UFPL are aware that no loan accounts will be created unless the KYC procedures are adhered to completely.

The Company through its Internal Audit Team will directly evaluate and ensure adherence to the KYC & AML policy and procedures, including legal and regulatory requirements. The Internal Audit department of the Company is tasked with checking the robustness of this Policy while carrying out their audits. Responsibility has also been explicitly allocated within the company for ensuring that the company's policies and procedures are implemented effectively. The nature and extent of due diligence will depend on the risk perceived by the branch/company. However, while preparing customer profile branches should take care to seek only such information from the customer which is relevant to the risk category and is not intrusive

Enhanced Due Diligence:

The Company is primarily engaged in lending. It does not deal with such category of customers who could pose a potential high risk of money laundering, terrorist financing or political corruption and are determined to warrant enhanced scrutiny. The Company shall conduct Enhanced Due Diligence in connection with all customers or accounts that are determined to pose a potential high risk and are determined to warrant enhanced scrutiny. Enhanced Due Diligence shall be coordinated and performed by the Company, who may engage appropriate outside investigative services or consult appropriate vendor sold databases when necessary. Business vertical shall establish procedures to decline to do business with or discontinue relationships with any customer when the Company cannot adequately complete necessary Enhanced Due Diligence or when the information received is deemed to have a significant adverse impact on reputational risk.

The following are the indicative list where the risk perception of a customer may be considered higher:

i. Customers requesting for frequent change of address/contact details
ii. Sudden change in the loan account activity of the customers
iii. Frequent closure and opening of loan accounts by the customers

Enhanced due diligence may be in the nature of keeping the account monitored closely for a re-categorization of risk, updating of fresh KYC documents, field investigation or visit of the customer, etc., which shall form part of the credit policies of the businesses.

Monitoring of Transactions-

The Company should exercise ongoing due diligence with respect to the business relationship with every customer and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, her business and risk profile and wherever necessary, the source of funds. Monitoring clients' activities and transactions that take place throughout a relationship helps the Company to know their customers, assess risk and provides greater assurance that the Company is not being used for the purposes of financial crime. Thus, monitoring means analysis of a customer transactions to detect whether the transactions appear to be suspicious from an AML perspective.

Suspicious Transactions

A suspicious transaction is one for which there are reasonable grounds to suspect that the transaction is related to a money laundering offence or a terrorist activity financing offence. A suspicious transaction can include one that was attempted. There is no monetary threshold for making a report on a suspicious transaction. A suspicious transaction may involve several factors that may on their own seem insignificant, but together may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering offence, a terrorist activity financing offence, or both. An illustrative (but not exhaustive) list of suspicious transactions is furnished in "Annexure-III".

The Company shall endeavor to put in place automated systems for monitoring transactions to identify potentially suspicious activity. Such triggers will be investigated and any suspicious activity will be reported to Financial Intelligence Unit-India (FIU-IND). The Company shall file the Suspicious Transaction Report (STR) to FIU-IND after arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.

Being an NBFC, the Company 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 customer, necessary forms would be filed with FIU-IND. The Principal Officer - PMLA would file the Counterfeit Report (STR) with the Director, Financial Intelligence Unit-India (FIU-IND) within the timeline prescribed under the Rules.

Cash Transaction Reports (CTR)

All individual cash transactions in an account during a calendar month, where either debits or credit summation, computed separately, exceeding Rupees Ten Lakhs or its equivalent in foreign currency, during the month should be reported to FIU-IND. However, while filing CTR, details of individual cash transactions below Rupees Fifty Thousand may not be indicated. The Principal Officer should ensure submission of CTR for every month to FIU-IND before 15th of the succeeding month. CTR should contain only the transactions carried out by the Company on behalf of their clients/customers excluding transactions between the internal accounts of the Company

Money Laundering and Terrorist Financing Risk Assessment by REs:

The Company will carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise annually to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, geographic areas, products, services, transactions or delivery channels, etc. The internal risk assessment carried out by the Company should commensurate to its size, geographical presence, complexity of activities/structure, etc. and shall apply a Risk Based Approach for mitigation and management of the identified risks. Respective businesses shall have standard operating procedures for identification, mitigation, controls and procedures for management of the identified risk, if any. The risk assessment processes shall be reviewed annually to ensure its robustness and effectiveness. The outcome of the exercise shall be put up to the risk management committee of the Board and should be available to competent authorities and self-regulating bodies

Updation / Periodic Updation of KYC

Updation of KYC shall be done at least every two years for high-risk customers, every eight years for medium risk customers and every ten years for low-risk customers from the date of opening of account/ last KYC updation. The company shall obtain self-declaration from Individual customers and non-Individual customers in case of no change in their KYC details. However, in case of change in address of individual customer a self-declaration of such change and proof of new address to be obtained and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc. In case of change in KYC information of non-individual customer, the Company shall undertake a KYC process which shall be equivalent to on-boarding a new customer.

Record Keeping:

Maintenance of records of transactions: As unlikely as it will be in the Company's case, due to its focus on lower income individuals, the Company has a system of maintaining proper record of transactions prescribed Section 12 of the PMLA read with Rule 3 of the Prevention of Money Laundering Rules, 2005 (PML Rules) as mentioned below:

a) All cash transactions of the value of more than Rupees Ten Lakhs (Rs. 10,00,000/-) or its equivalent in foreign currency, though by policy the Company neither accepts cash deposits nor transactions in foreign currency.

b) All series of cash transactions integrally connected to each other which have been valued below Rs. 10,00,000/- (Rupees Ten Lakhs) or its equivalent in foreign currency where such series of transactions have taken place within a month.

c) All transactions involving receipts by non-profit organizations of Rs. 10,00,000/- (Rupees Ten Lakhs) or its equivalent in foreign currency.

d) All cash transactions, where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place; any such transactions.

e) All suspicious transactions whether or not made in cash and in manner as mentioned in the PML Rules framed by the Government of India under PMLA. An Illustrative List of suspicious transaction pertaining to financial services is given in Annexure II.

Records to contain the specified information: The Records referred to above in Rule 3 of PML Rules to contain the following information:

a) The nature of the transactions;
b) The amount of the transaction and the currency in which it was denominated;
c) The date on which the transaction was conducted;
d) The parties to the transaction.

Maintenance and preservation of records: The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules

a) maintain all necessary records of transactions between the Company and the customer, for at least five years from the date of transaction;
b) preserve the records pertaining to the identification of the customers and their addresses obtained during the course of business relationship, for at least five years after the business relationship is ended;
c) The above records shall be maintained either in hard or soft format and shall be made available to the competent authorities upon request;

Appointment of Designated Director & Principal Officer

Mr. Hanumant Ranjane, Director of the Company has been appointed as "Designated Director" in compliance with of the Prevention of Money laundering (Amendment) Act, 2012 in terms of RBI Circular No. DNBS (PD) CC.No. 378/03. 10.42/ 2012-13 dated May 29, 2014 and Mr. Abhijit Ranjane, Managing Director has been designated as 'Principal Officer'.

Reporting of information with the FIU-IND

The Principal Officer will report information relating to cash and suspicious transactions if detected, to the Director, Financial Intelligence Unit-India (FIU-IND) as advised in terms of the PMLA rules, in the prescribed formats as designed and circulated by RBI.

The employees of the Company shall maintain strict confidentiality of the fact of furnishing/ reporting details of suspicious transactions.

Secrecy Obligations and Sharing of Information:

a) The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the Company and customer.
b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.
c) While considering the requests for data/information from Government and other agencies, the Company shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.
d) The exceptions to the said rule shall be as under:
   i. Where disclosure is under compulsion of law
   ii. Where there is a duty to the public to disclose,
   iii. the interest of the Company requires disclosure and
   iv. Where the disclosure is made with the express or implied consent of the customer.

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

The Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, RBI Direction issued from time to time, as required by the KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be.

Customer Education

The Company may regularly educate the customer of the objectives of the KYC programmed. The Company on an ongoing basis educates its employees, the branch staff and the new joiners on the elements of KYC through training programmers/e-mail.

Hiring & Training of Employees:

The Company shall have adequate screening mechanism as an integral part of their personnel recruitment/ hiring process. As part of induction process, employees of the Company are trained in KYC guidelines through training module.

The Company shall endeavor to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. REs shall also strive to develop an environment which fosters open communication and high integrity amongst the staff

Updating and modifications, if any, in the guidelines are also cascaded to the entire team to keep them abreast of the changes. On-going employee training shall be provided to the employees to adequately train them in AML / CFT and KYC procedures, related policies, regulations and issues

Assessment and Review:

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

Annexure I – KYC documents to be verified for Individual customers

Proof of identity/existence	• UID / Voter ID • PAN Card • Passport • Driving License • Scheduled Bank passbook with applicant's photograph on the same which is duly attested by bank officials. The respective account should be active. • Letter issued by the Mandal Officer/Revenue Officer/ Village Administrative Officer. • KYC documents' photocopies only need to be taken. (Originals not required) • KYC documents must be self-attested by applicant and co-applicant respectively.
Address proof	• Voter ID • UID • Driving License • Passport • Electricity, Telephone, Water bills –not older than 90 days • Other Utility Bills - not older than 90 days • Life Insurance Policy or latest Premium receipt • Rent agreement • Consumer Gas Connection Card/Book • House Allotment letter from Government organizations • Bank statements / Passbook cover page with address being mentioned • Photocopies of the documents should be self-attested by the respective person. BRM should ensure that the address mentioned is matching with the current address of customer. If customer is living in a rented house, then ensure the proof of their permanent address.

Annexure II- Illustrative List Of Suspicious Transaction Pertaining To Financial Services

Broad categories of reason for suspicion and examples of suspicious transactions for Non- Banking Financial Companies are indicated as under:

1. **Identity of client:**
   a) False identification documents
   b) Identification documents which could not be verified within reasonable time

c) Accounts opened with names very close to other established business entities.

2. Background of Client:

Suspicious background or links with known criminals.

3. Multiple Accounts:

a) Large number of accounts having a common account holder, introducer or authorized signatory with no rationale:
b) Unexplained transfers between multiple accounts with no rationale.

4. Activity in accounts:

a) Unusual activity compared with past transactions- Sudden activity in dormant accounts;
b) Activity inconsistent with what would be expected from declared business.

5. Nature of transactions;

a) Unusual or unjustified complexity;
b) No economic rationale or bonafide purpose;
c) Frequent purchases of drafts or other negotiable instruments with cash;
d) Nature of transactions inconsistent with what would be expected from declared business.

6. Value of Transactions:

a) Value just under the reporting threshold amount in an apparent attempt to avoid reporting.
b) Value inconsistent with the client's apparent financial standing.

7. Illustrative list of Suspicious Transactions:

a) Reluctant to part with information, data and documents;
b) Submission of false documents, purpose of loan and detail of accounts;
c) Reluctance to furnish details of source of funds of initial contribution;
d) Reluctance to meet in person, representing through power of attorney;
e) Approaching a distant branch away from own address;
f) Maintaining multiple accounts without explanation;
g) Payment of initial contribution through unrelated third-party account;
h) Suggesting dubious means for sanction of loan;
i) Where transactions do not make economic sense;
j) Where doubt about beneficial ownership;
k) Encashment of loan through a fictitious bank account;
l) Sale consideration quoted higher or lower than prevailing area prices;
m) Request for payment in favor of third party with no relation to transaction;
n) Usage of loan amount for purposes other than stipulated in connivance with vendors, or agent;
o) Multiple funding involving NGO, Charitable organization, small and medium establishments, self-help groups, micro finance groups, etc.;
p) Frequent request for change of address;
q) Over-payment of installments with a request to refund the overpaid.