KYC AND AML POLICY

Of

FDPL FINANCE PRIVATE LIMITED

(FFPL)

Approval Date	Version History	Approval Authority
28th Jan 2023	V-FY2201	Board of Directors
15th Jan 2025	V-FY2401	Board of Directors

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

Introduction

FDPL Finance Private Limited is a private limited company, incorporated under the provisions of the Companies Act, 2013, having Corporate Identification Number (CIN) U65929MH2022PTC376853 ("FFPL" / "Company"), and is registered with Reserve Bank of India ("RBI") as a non-banking financial company ("NBFCs"), bearing Registration no. N-13.02471 and regulated by the RBI Directions as applicable to NBFCs and such other rules, regulations, directions, circulars, notifications and orders issued in this regard from time to time.

FFPL is into the business of providing consumer and personal loans.

1. PREAMBLE

RBI has issued comprehensive 'Know Your Customer' ("KYC") Guidelines to all NBFCs in the context of the recommendations made by the Financial Action Task Force ("FATF") on Anti Money Laundering ("AML") standards and Combating Financing of Terrorism ("CFT") policies, as these are used as the International Benchmark for framing the stated policies, by the regulatory authorities. In view of the same, the Company has adopted this Policy with suitable modifications depending on the activity undertaken by it. The Company has ensured that a proper policy framework on KYC and AML measures are formulated in line with the prescribed RBI Directions (this "Policy") and duly approved by its Board of Directors ("Board").

This Policy has been framed in accordance with the Master Directions – Know Your Customer (KYC) Direction, 2016 issued vide RBI Circular No. DBR.AML.BC. No.81/ 14.01.001/2015-16 dated February 25, 2016 updated as on October 17, 2023 and subsequent modification thereof ("Master Direction on KYC and AML"). As a Base Layer NBFC, FFPL adopts a proportionate approach to implementing KYC and AML obligations. Implementation shall be commensurate with the Company's size, nature, complexity, and risk profile, while ensuring full regulatory compliance

2. DEFINITION

2.1	Customer	1. a person or an entity who has a business relationship with the Company; 2. a person who avails financial assistance from the Company; 3. one on whose behalf the account is maintained (i.e. the beneficial owner where the term "beneficial owner" shall have the meaning assigned to it under the Master Direction on KYC and AML);
2.2	"Customer Due Diligence (CDD)"	means identifying and verifying the customer using reliable and independent sources of identification.
2.3	Customer identification"	"means undertaking the process of CDD
2.4	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
2.5	"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 PML Act.

2.6	"Digital Signature	As defined in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
2.7	Designated Director	"Designated Director" means a person designated by the Board to ensure overall compliance with the obligation imposed under chapter IV of the Prevention of Money Laundering ("PML") Act, 2002 ("PML Act") and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 ("PML Rules").
2.8	Equivalent e-document	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.
2.9	Equivalent e-document of any OVD	Equivalent e-document of any OVD" means an electronic version of an OVD obtained from the DigiLocker system of a customer.
2.10	KYC Identifier	KYC Identifier" means the unique number or code assigned to a customer by the Central KYC Records Registry.
2.11	Money Laundering	Money Laundering" has the meaning assigned to the term "offence of money- laundering" under Section 3 of the PML Act.
2.12	Officially valid document	Officially valid document" ("OVD") means (i) the passport; (ii) the driving license; (iii) proof of possession of Aadhaar number; (iv) the Voter's Identity Card issued by the Election Commission of India; (v) job card issued by NREGA duly signed by an officer of the State Government; and (vi) 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 or the equivalent e-documents thereof shall be deemed to be the 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 or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license 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.

2.13. "On-going Due Diligence" means regular monitoring of transactions in accounts to ensure that those are consistent with RE's knowledge about the customers, customers' business and risk profile, the source of funds / wealth.

2.14. "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.

2.15. "Principal Officer" means an officer at the management level nominated by the Board, responsible for furnishing information and such other obligations as applicable under the PML Act and the PML Rules, including the information specified under Rule 8 of the PML Rules.

2.16. "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:

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or

b. appears to be made in circumstances of unusual or unjustified complexity; or

c. appears to not have economic rationale or bona-fide purpose; or

d. 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.

2.17. "Transaction" is defined as:
A purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

2.17.1. opening of an account;

2.17.2. deposits, 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;

2.17.3. the use of a safety deposit box or any other form of safe deposit;

2.17.4. entering into any fiduciary relationship;

2.17.5. any payment made or received in whole or in part of any contractual or other legal obligation;

2.17.6. any payment made in respect of playing games of chance for cash or kind including such activities associated with casino; or

2.17.7. establishing or creating a legal person or legal arrangement.

2.18. All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, the Reserve Bank of India Act, 1934, the PML Act, the PML Rules, the Master Direction on KYC and AML (as applicable) and any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

2.19. "Video based Customer Identification Process (V-CIP)": an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the RE by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this Master Direction. Further, in case the amount of loan to be sanctioned is equivalent to or exceeds Rs. 1,00,000, it is mandatory to complete the KYC process using V-CIP.

KYC REQUIREMENT:

3.1. Customer Acceptance Policy ("CAP") is covered in Annexure-1.

3.2. Customer Identification Procedures ("CIP") are given in Annexure-2.

3.3. CDD Procedures

3.3.1 CKYCR Procedure:

The Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be, and as updated from time to time by CERSAI. The Company shall upload the KYC data pertaining to all new individual accounts opened on or after April 1, 2017, with the CKYCR in terms of the provisions of the PML Rules ibid. The Company shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to a RE, with an explicit consent to download records from CKYCR, then such RE shall retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless:

(i) there is a change in the information of the customer as existing in the records of CKYCR;

(ii) the current address of the customer is required to be verified;

(iii) the Company considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client; or

(iv) the validity period of documents downloaded from CKYCR has lapsed.

The Company shall upload/update the KYC data pertaining to accounts of individual customers and LEs at the time of periodic updation or earlier when the updated KYC information is obtained/received from the customer.

Refer Annexure-3 for detailed CDD procedure.

3.3.2 Digi Locker Procedure:
The Company also collects the PAN and an equivalent e-document of an OVD containing the details of a customer's identity and address, which is mapped and further verified through a live photograph of the Customer along with geo-mapping. During this process, the Company complies with the Master Direction on KYC and AML.

3.4. Record Management is covered in Annexure-4.

3.5. Risk Management is covered in Annexure-5.

3.6. Enhanced Due Diligence (EDD) measures is covered in Annexure-6

3.7. Appointment of Principal Officer
The Company shall appoint a Principal Officer, who shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. The Principal Officer will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

The Principal Officer shall report quarterly to the Board / Audit Committee on AML and KYC compliance, red-flag indicators, and STR/CTR submissions.

3.8. Appointment of Designated Director
The Company shall appoint a Designated Director in terms of the obligations under applicable laws, PML Act and clarification issued vide RBI Circular DNBR.PD.CC.No.022/03.10.042/2014-15 dated March 16, 2015 and subsequent modification thereof.

The Board of Directors shall review the implementation of this Policy and AML/KYC compliance at least annually, and approve any amendments required.

3.9. Ongoing Due Diligence:
The Company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with its knowledge about the customers, customers' business and risk profile; and the source of funds including cash / wealth. Among other things, following types of transactions shall necessarily be monitored, as may be applicable:

• Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.

• Transactions, which exceed the thresholds prescribed for specific categories of accounts.

• High account turnover inconsistent with the size of the balance maintained.

• Deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

Monitoring of transactions and its extent will be conducted taking into consideration the risk profile of the account. The Company shall make endeavours to understand the normal and reasonable activity of the Customer so that the transactions that fall outside the regular/pattern of activity can be identified, special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose. The Company shall have a Management approved standard operating procedure (SOP) to categorize cases as High, Medium, Low Risk.

FIU-IND has released a Guidance Note on Transaction Monitoring for NBFCs, which is applicable to the Company as well. Vide the said note, FIU-IND has prescribed certain Red Flag Indicators (RFIs) which are required to be implemented by NBFC for the purpose of generation of alerts to ensure effective transaction monitoring. The Company shall implement these RFIs suitably as may be applicable to its line of business. Appropriate thresholds shall be set considering the risk categorization of customers that will ensure intensified monitoring for its customers. While reviewing the alerts, attention shall be paid to the background of the customer, customer's identity, social/financial status, nature of business activity,

country of origin, sources of funds, geographical risk, the type of transactions involved, 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. Since all the accounts are classified as high-risk accounts and are required to be subjected to EDD, there is no requirement for the company to carry out periodic review of risk categorization of transactions/customer's accounts.

In order to comply with Chapter IX of the Master Direction on KYC and AML, the Company uses a database provided by vendor for the purpose of screening new account opening applications against certain watch lists, including the ones prescribed by RBI. In case of a true match is identified, apart from preventing the customer on-boarding, the company performs necessary reporting to FIU-IND, MHA, Central Nodal Officer (CNO), State Nodal Officer and RBI in line with the UAPA, WMD notification, order.

The lists are updated periodically by the vendor and the screening is performed even at the time of fresh loan disbursement for an existing customer. The Company shall also undertake countermeasures when called upon to do so by any international or intergovernmental organization of which India is a member and accepted by the Central Government.

The Risk Assessment exercise is required to be carried out periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas shall not be applicable to the Company considering all the relevant risk factors and the level of overall risk basis its products, services, ticket size of its transactions, delivery channels, etc. The periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. However, it would be reviewed at least annually.

The Company shall adopt a Risk Based Approach (RBA) to classify customers into Low, Medium, and High-risk categories based on parameters such as nature of business, mode of on-boarding, geography, transaction pattern, and product type. The same shall be adopted for mitigation and management of the risks (identified on its own or through national risk assessment). The Company shall implement a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, the Company shall monitor the implementation of the controls and enhance it, if necessary, at the time of review of the risk assessment.

FFPL shall proactively educate customers regarding the purpose of KYC, the need for periodic updates, their rights under PMLA/DLG, and grievance redressal mechanisms. Such information shall be made available on the Company's website, onboarding documentation, and customer agreements.

3.10. Reporting of Transactions:
Further, Company shall be guided by RBI's advice for necessary actions to be taken, including additional measures (if any) for managing the ML/TF risk(s), in case applicable laws and regulations prohibit implementation of the Master Direction on KYC & AML. In accordance with the requirements under PML Act, the Principal Officer will furnish certain reports within the prescribed timelines to the Director, Financial Intelligence Unit- India (FIU-IND). The reporting requirements and their applicability to the Company are as below:

3.10.1. Cash transaction report (CTR) for each month should be submitted to FIU- INDIA by 15th of the succeeding month. However, it is notable that this requirement is not applicable, for the time being, to the Company as the Company does not accept cash as a mode of loan repayment beyond the prescribed reporting threshold.

3.10.2. Counterfeit Currency Report (CCR) – All such cash transactions where forged or counterfeit Indian currency notes have been used as genuine as Counterfeit Currency Report (CCR) for each month by 15th of the succeeding month.

3.10.3. NPO Transaction Report (NTR) – all transactions involving receipts by non-profit organizations of value more than rupees ten lakh, or its equivalent in foreign currency. This is not applicable to the Company as it is into the business of lending and NPO is not a target market segment for the company.

3.10.4. Cross Border Wire Transfer Report (CBWTR) – all cross-border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India. This is not applicable to the Company as there are no cross-border flow of funds either for receiving or for remittance except through its bank accounts.

3.10.5. Suspicious Transactions Reporting (STR) – Report on suspicious transaction(s), whether cash or non-cash, or a series of transactions integrally connected that are of suspicious nature, shall be filed within 7 days of arriving at a conclusion that the transaction(s) are suspicious.

The Company shall undertake on-going due diligence, as explained above, to identify and report suspicious activity / transaction(s). However, in accordance with the regulatory requirements, the Company will not be able to put any restriction on operations in the accounts where an STR has been filed, since it is into lending business. However, it will ensure not to disburse any fresh loan to the customers on whom STRs have been filed, albeit without tipping off to the customer about filing of STR.

3.11. Training Programme:
The Company will have an ongoing employee training program so that the members of the staff are adequately trained in KYC/ AML procedures and are updated with the changing KYC/AML/CFT landscape, nationally and internationally.

Training program shall take into consideration the requirements, which are different in terms of the focus for frontline staff, compliance staff and officer/ staff dealing with new customers so that all those concerned fully understand the rationale behind the KYC policies / norms and implement them consistently.

V-CIP should only be carried by specifically trained officials of the Company who should be capable of carrying out liveness checks as also other parameters and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

3.12. Internal Control System:
The Company's Internal Audit and Compliance functions will evaluate and ensure adherence to the KYC policies and procedures. As a general rule, the compliance function will provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements.

The Management under the supervision of RMC is ensuring that the audit of this aspect is part of the scope of work of internal auditors, besides ensuring that internal audit department is staffed adequately with skilled individuals. Internal Auditors will specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The audit findings and compliance thereof will be put up before the Audit Committee by the RMC on quarterly intervals till closure of audit findings.

Any suspected breach of AML/KYC obligations may also be reported under the Company's Vigil Mechanism / Whistle-blower framework, ensuring confidentiality and protection from retaliation.

Further, the Company shall have an adequate screening mechanism in place as an integral part of their recruitment/ hiring process of personnel so as to ensure that person of criminal nature/ background do not get an access, to misuse the financial channel.

3.13. The Principal Officer after taking the due approval from the Board shall make the necessary amendments/modifications in this Policy or such other related guidance notes of Company, to be in line with RBI or such other statutory authority's requirements/updates/ amendments from time to time.

Annexure-1

Customer Acceptance Policy

1. The Company shall ensure that:

1.1. No account shall be opened by Company in anonymous or fictitious/benami names.

1.2. No account shall be opened where 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. The Company shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.

1.3. No transaction or account-based relationship is undertaken without following the CDD procedure.

1.4. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation shall be as specified by this Policy and as amended or specified from time to time. Any exceptions shall be discussed with the Principal Officer.

1.5. Additional information, where such information requirement has not been specified in this Policy, shall be obtained only with the explicit consent of the customer.

1.6. Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the lists mentioned under paragraph 3.9 hereinabove.

1.7. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority / NSDL.

1.8. Where an equivalent e-document is obtained from the customer, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).

1.9. If the customer or the beneficial owner is Politically Exposed Persons (PEP), then the same shall be specifically highlighted to the Principal Officer and the Designated Director as also to RMC for their approvals.

2. The Company undertakes that this customer acceptance policy shall not result in denial of banking/financial facility to members of the general public, especially those who are financially or socially disadvantaged.

3. Where the company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, but instead file an STR with FIU-IND.

Annexure-2

PART A

Customer Identification Procedures

Customer identification shall be undertaken at the time of commencement of an account-based relationship which includes identifying the Company's customers, verifying their identities, obtaining information on the purpose and intended nature of the business relationship; and determining whether a client is acting on behalf of a beneficial owner, and identify the beneficial owner and take all steps to verify the identity of the beneficial owner.

Accounts opened using OTP based e-KYC shall not be allowed for more than one year. In case, the Company decides to conduct digital KYC, it shall develop an application for its 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. The Company would ensure to adhere to the procedure and practice as prescribed by RBI in the Master Directions on KYC/AML, as per paragraph 10 hereinbelow.

1. The Company shall undertake identification of customers in the following cases:

1.1. Commencement of an account-based relationship with the customer;

1.2. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained;

1.3. Selling their own products, selling third party products as agents and any other product for more than INR 50,000/- (Indian Rupees Fifty Thousand only);

1.4. Carrying out transactions for a non-account-based customer (walk-in customer).

Further, the Company shall ensure that introduction is not to be sought while opening accounts.

2. The Company shall obtain satisfactory evidence of the identity of the customer depending upon the perceived risks at the time of commencement of relationship/ opening of account. Such evidence shall be substantiated by reliable independent documents, data or information or other means like physical verification etc. The Company can also undertake 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 by using reliable and independent sources of identification

3. For undertaking CDD, company shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

(a) the Aadhaar number where, he decides to submit his Aadhaar number voluntarily notified under first proviso to sub-section (1) of section 11A of the PML Act; or

(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

(ab) 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; or

(ac) the KYC Identifier with an explicit consent to download records from CKYCR; and

(b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

(c) 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.

4. Aadhaar number submitted under clause above notified under first proviso to sub-section (1) of section 11A of the PML Act, company shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the RE.

Proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the RE shall carry out offline verification.

An equivalent e-document of any OVD, the company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Annex I.

Any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the company shall carry out verification through digital KYC as specified under Annex I of Master Direction.

KYC Identifier under clause (ac) above, the company shall retrieve the KYC records online from the CKYCR in accordance with Section 56.

5. Additional documentation may be obtained from the customers with higher risk perception as may be deemed fit. This shall be done having regard but not limited to location (registered office address, correspondence address and other addresses as may be applicable), nature of business activity, monitoring of transactions in the account, repayment mode & repayment track record.

6. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, the Company may, at its discretion, rely on customer due diligence done by a third party, subject to the following conditions:

6.1. Necessary information of such customers' due diligence is immediately obtained by the Company from the third party or from the Central KYC;

6.2. Adequate steps are taken by the Company to satisfy that the copies of identification data and other relevant documentation relating to customer due diligence shall be made available from the third party upon request without delay

6.3. The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act;

6.4. The third party shall not be based in a country/ jurisdiction assessed as high risk;

6.5. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures (as per Annexure-6), as applicable, will be with the Company.

7. While undertaking customer identification, the Company will ensure that:

7.1. Decision-making functions of determining compliance with KYC norms shall not be outsourced.

7.2. The customers shall not be required to furnish an additional OVD, if the OVD or equivalent e-document of the OVD submitted for KYC contains proof of identity as well as proof of address e.g., Passport.

7.3. The customers will not be required to furnish separate proof of address for permanent and current addresses, if these are different. In case the proof of address furnished by the customer is the address where the customer is currently residing, a declaration shall be taken from the customer about her/ his local address on which all correspondence will be made by the Company. The local address for correspondence, for which their proof of address is not available, shall be verified through 'positive confirmation' such as address verification letter, contact point verification, deliverables, etc.

7.4. In case of change in the address mentioned on the 'proof of address', fresh proof of address should be obtained within a period of two (2) months.

7.5. A Unique Customer Identification Code (UCIC) is allotted while entering into new relationships with individual Customers by the Company. The Company uses the PAN hash value as UCIC.

8. Periodic Updation of KYC data
The company shall ensure to carry out periodic updation at least once in every two years for high-risk customers, once in every eight years for medium risk customers and once in every ten years for low-risk customers from the date of opening of the account / last KYC updation. The below approach shall be followed for periodic updation:

• No change in KYC information: In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's registered email-id, customer's registered mobile number, digital channels (such mobile application), letter, etc.

• Change in address: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's registered email-id, customer's registered mobile number, digital channels (such mobile application), letter, etc., and the declared address shall be verified through positive confirmation within two months, by means mentioned in para 8.3 hereinabove.

Further, PAN and Aadhaar verification from DigiLocker is done by the Company in case of a change in address.

In addition to the above, the Company shall ensure that:

• The KYC documents of the customer as per the current CDD standards are available and that the information or data collected under CDD is kept up-to-date and relevant. This is applicable even if there is no change in customer information but the documents available are not as per the current CDD standards. Further, in case the validity of the CDD documents available has expired at the time of periodic updation of KYC, the KYC process equivalent to that applicable for on-boarding a new customer shall be undertaken.

• Customer's PAN details, is verified from the database of the issuing authority at the time of periodic updation of KYC.

• Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

9. The Company shall advise the Customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the Customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary, Customers shall submit to the Company the update of such documents within 30 (thirty) days of such updation.

10. Digital KYC Process

While carrying out a Digital KYC, the Company shall adhere to the following requirements:

10.1 The Company shall develop an application to conduct 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. The Company would ensure to adhere to the procedure and practice as prescribed by RBI in the Master Directions on KYC/AML.

10.2 The access of the application shall be controlled by the Company and it should be ensured that it is not used by any unauthorized person. 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.

10.3 The Company shall 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 the Company) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

10.4 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 shall be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.

10.5 The live photograph of the customer shall be captured in proper light so that it is clearly identifiable.

10.6 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.

10.7 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 Company shall not be used for customer signature. The Company must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

10.8 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 Company. 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.

10.9 The authorized officer of the Company 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.

11. In line with the RBI Digital Lending Guidelines (September 2022), FFPL shall ensure that:

- All disbursals are made only into the borrower's bank account and repayments are received only from the borrower's bank account, without any pass-through arrangements.
- Data collected during KYC and lending processes shall be used only with the borrower's explicit consent and for disclosed purposes.
- Any engagement with Lending Service Providers (LSPs) shall comply with RBI norms on data storage, sharing, and auditability.
- All First Loss Default Guarantee (FLDG) arrangements, where applicable, shall be transparently documented and comply with RBI's prudential norms.

PART B

Video based Customer Identification Process ("V-CIP")
The Company must adhere to following minimum standards in respect of V-CIP (in case it is opting to undertake V-CIP):

1. V-CIP Infrastructure

The Company's V-CIP infrastructure shall be compliant with the Master Direction for KYC and AML and other relevant statutes in the manner including but not limited to stated hereunder:

1.1 The Company shall ensure the relevant RBI guidelines are adhered to as a minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. Also, the Company shall ensure that the technology infrastructure should be housed in own premises of the Company and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology-related outsourcing for the process should be compliant with relevant RBI guidelines.

1.2 The Company shall ensure that wherever cloud deployment model is used, the ownership of data in such model rests shall rest with the Company only and all data including video recording shall be transferred to the Company's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Company.

1.3 The Company shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. Customer consent should be recorded in an auditable and alteration-proof manner.

1.4 The Company shall ensure that the V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

1.5 The video recordings should contain the live GPS co-ordinates (geo-tagging) of the Customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

1.6 The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Company. Appropriate artificial intelligence (AI) technology can be used to ensure that V-CIP is robust.

1.7 Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as workflows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

1.8 The Company shall ensure that the V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation.
Such tests should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). The Company shall ensure that such tests carried out periodically in conformance to internal/regulatory guidelines.

1.9 The Company shall ensure that the V-CIP application software and relevant APIs / webservices shall undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically.

2. V-CIP Procedure

2.1 The Company shall formulate a clear workflow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the Company trained for this purpose.

2.2 Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption does not lead to the creation of multiple files, then there is no need to initiate a fresh session by the Company. However, in case of call drop / disconnection, fresh session shall be initiated.

2.3 The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre-recorded.

2.4 The Company shall ensure that any prompting observed at end of Customer shall lead to rejection of the account opening process.

2.5 The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in appropriate stage of work-flow.

2.6 The authorized official of the Company performing the V-CIP shall record audio-video as well as capture photograph of the Customer present for identification and obtain the identification information using any one of the following:

(i) OTP based Aadhaar e-KYC authentication;

(ii) Offline Verification of Aadhaar for identification;

(iii) KYC records downloaded from CKYCR, in accordance with Section 56, using the KYC identifier provided by the customer; or

(iv) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker.

2.7 The Company shall ensure to redact or blackout the Aadhaar number in terms of Section 16 of the Master Direction on KYC and AML.

2.8 In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, the Company shall ensure that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP.

2.9 Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, the Company shall ensure that the video process of the V-CIP is undertaken within three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, the Company shall ensure that no incremental risk is added due to this.

2.10 If the address of the Customer is different from that indicated in the OVD or electronic version thereof, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the Customer is also confirmed from the Customer undertaking the V-CIP in a suitable manner.

2.11 The Company shall capture a clear image of 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 NSDL/ Protean eGov Technologies Limited including through DigiLocker.

2.12 Use of printed copy of equivalent e-document including e-PAN shall not be considered valid for V-CIP by the Company.

2.13 The authorized official of the Company shall ensure that photograph of the Customer in the Aadhaar/OVD and PAN/e-PAN matches with the Customer undertaking the V- CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the Customer.

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

2.15 All matters not specified here but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied.

3. V-CIP Records and Data Management

3.1 The entire data and recordings of V-CIP shall be stored in a system / systems located in India. The Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management are stated in Annexure 4.

3.2 The activity log along with the credentials of the official performing the V-CIP shall be preserved by the Company.

Annexure-3

Customer Due Diligence Procedures

PART – A
For undertaking CDD, the Company shall obtain the following while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:
(a) Aadhaar Number, OR

(b) The proof of possession of Aadhaar number where offline verification can be carried out, OR

(c) 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, OR

(d) The KYC Identifier with an explicit consent to download records from CKYCR; and

(e) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

(f) 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 RE Accounts opened using

Aadhaar OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:

(a) There must be specific consent from the customer for authentication through OTP.

(b) As a risk-mitigating measure for such accounts, it shall be ensured that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. Company shall deal with requests for change of mobile number in such accounts, as mentioned in paragraph 2 of Part B hereinbelow.

(c) Only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.

(d) Accounts opened using OTP based e-KYC shall not be allowed for more than one year unless identification as detailed above or as per V-CIP (Annexure II, Part B above) is carried out. If Aadhaar details are used under V-CIP, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

(e) If the CDD procedure mentioned above is not completed within a year, no further disbursals shall be allowed.

(f) 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 in non-face-to-face mode with any other RE. Further, while uploading KYC information to CKYCR, Company shall clearly indicate that such accounts are opened using OTP based e-KYC so that other REs would not open accounts

1. Company to carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect.

2. Company to carry out offline verification.

3. Any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, Company to carry out verification through digital KYC.

4. Includes the passport, the driving license, 13proof 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

5. Company to verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo.

6. Company to retrieve the KYC records online from the CKYCR. Based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

The company shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above-mentioned conditions.

PART – B

Enhanced Due Diligence ("EDD") for non-face-to-face customer onboarding

The Company shall undertake non-face-to-face onboarding of customers through the use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc.
In accordance with Paragraph 40 of the Master Direction on KYC and AML, the following EDD measures shall be undertaken by the Company for non-face-to-face customer onboarding through the digital channels mentioned above:

1. The Company shall ensure that any and all transactions shall be permitted only from the mobile number used for account opening. The Company shall not link alternate mobile numbers of Customers post CDD for transaction OTP, transaction updates, etc. Any request for a change to the mobile number has to be carried out in accordance with the process mentioned under sub- paragraph 2 below.

2. All requests for change of registered mobile number or updation of any documents shall only be carried out upon taking explicit consent of the Customer along-with PAN number of such Customer. All such requests shall only be entertained upon verification of the PAN number of the customer and no requests for re-change in mobile numbers shall be entertained within 24 (twenty-four) hours of receipt or the request or processing of the previous request.

3. In addition to obtaining the current address proof of the Customer through the digital channels mentioned above (viz. CKYCR, DigiLocker, equivalent e-document, etc.), the Company shall verify the current address through positive confirmation, as mentioned in para 8.3 hereinabove.

4. The Company shall obtain PAN from the Customers and shall verify such PAN from the verification facility of NSDL.

5. The company is required to disburse the loan amount to the customer's verified bank account, following confirmation through a penny drop by the bank.

6. The Company shall ensure that Customer(s) onboarded through non-face-to-face process i.e. digital channels mentioned above (viz. CKYCR, DigiLocker, equivalent e-document, etc.), shall be categorized as high-risk and such Customer's account shall be subjected to enhanced monitoring until the identity of the Customer is verified through face-to-face manner either physically or V-CIP.

Annexure-4

Record Management

1. The following steps shall be taken regarding maintenance, preservation and reporting of customer information, with reference to the provisions of the PML Act and Rules. The Company shall:

1.1. maintain all necessary records of transactions between the Company and the Customer including the walk-in customers, both domestic and international, for at least 8 (eight) years from the date of transaction;
The customer shall be provided with an option to give or deny consent for use of specific data, restrict disclosure to third parties, data retention, revoke consent already granted to collect personal data and if required, make the app delete/ forget the data, as provided for in Digital Lending Guidelines issued by RBI.

1.2. preserve the records pertaining to the identification of the Customers and their addresses obtained while opening the account and during the course of business relationship, for at least 5 (five) years after the business relationship is ended;

1.3. make available swiftly the identification records and Transaction data to the competent authorities upon request; where required by law enforcement agencies or in cases of ongoing investigations, records shall be retained for longer periods;

1.4. introduce a system of maintaining proper record of transactions prescribed under Rule 3 of the PML Rules so as to permit reconstruction of individual transaction, including the following:

1.4.1. the nature of the Transactions;

1.4.2. the amount of the Transaction and the currency in which it was denominated;

1.4.3. the date on which the Transaction was conducted; and

1.4.4. the parties to the Transaction.

1.5. evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;

1.6. maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 of the PML Rules in hard or soft format.

2. The Company, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director is confidential.

Annexure-5

Risk Management

1. For Risk Management, the Company will have a risk-based approach which includes the following:

1.1. Customers shall be categorized as low, medium and high-risk category, based on the assessment and risk perception of the Company;

1.2. 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 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 offline or other services offered by issuing authorities may also be factored in;

1.3. 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;

1.4. The various other information collected from Customers relating to the perceived risk, is non-intrusive.

Annexure-6

Enhanced Due Diligence (EDD) Measures

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

1.1. Company shall have in place appropriate risk management systems to determine whether the customer is a PEP.

1.2. Company shall gather sufficient information about the sources of funds / wealth.

1.3. The decision to provide financial services to an account for PEP shall be taken at a senior level.

1.4. All such accounts are subjected to enhanced monitoring on an on-going basis.

1.5. In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the continuance of the business relationship will be subject to the RMC's approval.

1.6. The above norms shall also be applied to the accounts of the family members or close relatives of PEPs.

2. Accounts of non-face-to-face customers

2.1. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk.

2.2. Certification of all the documents presented may be insisted upon and, if necessary, additional documents may be called for.

2.3. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the NBFCs may have to rely on third party certification/ introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.