PFSPL/FY2025-26/3.1

PAHAL FINANCIAL SERVICES PRIVATE LIMITED

Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy V3.1

PAHAL
A NEW BEGINNING

Table of Contents

1 Preamble

As a Non-banking Finance Company-Microfinance Institution (NBFC-MFI), registered with the Reserve Bank of India (RBI), PFSPL Financial Services Pvt. Ltd. (PFSPL) is required as per RBI guidelines to adopt "Know Your Customer & Anti-Money Laundering Policy."

The current version of the combined Policy on Know Your Customer (KYC) and Prevention of Money Laundering Activities (PMLA) is the updated version where a formal policy on PMLA has been integrated into the prevalent KYC Policy, duly edited in line with the latest guidelines of Reserve Bank of India.

The policy will comply with the Reserve Bank of India Master Direction on Know Your Customer Direction, 2016 vide notification number **RBI/DBR/2015-16/18 Master Direction DBR.AML.BC. No.81/14.01.001/2015-16** (Updated as of Aug 14, 2025) or any subsequent change in the notification/master direction.

The Policy will fall due for review yearly.

2 Objectives

The objective of KYC guidelines is:

1. To prevent PFSPL from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable PFSPL to know/understand customers and their financial dealings better, which in turn helps them manage their risks prudently.
2. To put in place systems and procedures to help control financial frauds, identify money laundering and suspicious activities, and safeguard PFSPL from being unwittingly used as a conduit for transferring or depositing funds derived from criminal activity or financing terrorism.
3. To put in place systems and procedures for customer identification and verifying their identity and address; and
4. To monitor transactions of a suspicious nature.

3 Applicability

The Policy applies to every business activity of PFSPL. Any contravention or non-compliance will attract a penalty for the company. Hence commensurate care and responsibility as regards compliance, including readiness to bear penalty for non-compliance, is expected from the employees of PFSPL.

4 Definitions

- **Customer**- A Customer is defined as a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
- **Person** - In terms of the PML Act a 'person' includes:
    i. an individual,

ii. a Hindu undivided family,
iii. a company,
iv. a firm,
v. an association of persons or a body of individuals, whether incorporated or not,
vi. every artificial juridical person, not falling within any one of the above persons (i to v), and
vii. any agency, office, or branch owned or controlled by any of the above persons (i to vi).

- **Act-** the Prevention of Money-Laundering Act, 2002.
- **Rules-** Prevention of Money-Laundering (Maintenance of Records) Rules, 2005
- **Unique Customer Identification Code (UCIC)-**
- **Designated Director-** A person designated by PFSPL to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules.
  The name, designation and address of the Designated Director shall be communicated to the FIU-IND.
  Further, the name, designation, address and contact details of the Designated Director shall also be communicated to the RBI.
  In no case, the Principal Officer shall be nominated as the 'Designated Director'.
- **Principal Officer-** An officer nominated by the RE, responsible for furnishing information as per rule 8 of the Rules.
  The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.
  Further, the name, designation, address and contact details of the Principal Officer shall also be communicated to the RBI.
- **Know Your Client (KYC)** Identifier means the unique number or code assigned to a customer by the Central KYC Records Registry.
- **Digital KYC** means capturing a live photo of the customer and an officially valid document or proof of possession of an Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where an authorized officer of the RE is taking such live photo as per the provisions contained in the Act.
- **Digital Signature** shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
- **Suspicious Transaction-** a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:
  i. give rise to a reasonable ground of suspicion that it may involve proceeds of an offense specified in the Schedule to the Act, regardless of the value involved.
  ii. appears to be made in circumstances of unusual or unjustified complexity.
  iii. appears to not have an economic rationale or Bonafide purpose.
  iv. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
- 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 the digital form of a customer.
- **Due Diligence (CDD)**- It means identifying and verifying the customer and the beneficial owner.
- **Politically Exposed Person (PEP)**- Individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

- **Shell bank** – It means a bank incorporated in a jurisdiction in which it has no physical presence, and which is unaffiliated with a regulated financial group.

5. Designated Authorities

5.1 Designated Director

"Designated Director" will be designated by PFSPL to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules and S/he will be nominated by the Board.

Name	Mr. Kartik Mehta
Designation	Managing Director
Phone	+91 2717 479169
Email	kartik.mehta@pahalfinance.com

5.2 Principal Officer

The Principal Officer will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

Name	Ms. Anubhuti Kapadia
Designation	Chief Compliance Officer
Phone	+91- 9588877844
Email	anubhuti.kapadia@pahalfinance.com

The Principal Officer will report the same to the Audit Committee.

6. Policy

The KYC policy includes the following four key elements:

A. Customer Acceptance Policy (CAP)
B. Risk Management
C. Customer Identification Procedures (CIP)
D. Monitoring of Transactions

6.1 Customer Acceptance Policy (CAP)

PFSPL has developed a clear Customer Acceptance Policy laying down explicit criteria for the acceptance of customers. The Customer Acceptance Policy shall ensure that explicit guidelines are in place on the following aspects of customer relationships in PFSPL.

1. No account is opened in an anonymous or fictitious/benami name. PFSPL will ensure that its customer is not a fictitious person by verifying the identity of the customer through documentation and will also carry out necessary checks, to ensure that the identity of the customer based on the documents obtained does not match with any person with known criminal background or with banned entities, such as individual terrorists or terrorist organizations. PFSPL

will periodically monitor its customer base with the RBI circulars and information providing such lists of terrorists or terrorist organizations.

2. No account is opened where the PFSPL is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.
3. No transaction or account-based relationship is undertaken without following the CDD procedure.
4. The mandatory information to be sought for KYC purposes while opening an account and during the periodic updation, is specified.
5. 'Optional'/additional information is obtained with the explicit consent of the customer after the account is opened.
6. PFSPL will apply the CDD procedure at the Unique Customer Identification Code (UCIC) level. Thus, if an existing KYC-compliant customer of PFSPL desires to open another account with the PFSPL, there shall be no need for a fresh CDD exercise.
7. Circumstances in which a customer is permitted to act on behalf of another person/entity is spelled out.
8. Where a Permanent Account Number (PAN) is obtained, the same shall be verified by the verification facility of the issuing authority.

The Customer Acceptance Policy of PFSPL will not result in the denial of financial facilities to members of the general public, especially those who are financially or socially disadvantaged.

6.2 Risk Management

- PFSPL will apply a Risk-Based Approach (RBA) for the mitigation and management of the identified risk and have policies, controls, and procedures in this regard. Further, PFSPL will monitor the implementation of the controls and enhance them if necessary.
- Under the Risk-Based Approach, customers will be categorized into 'High Risk', 'Medium Risk', and Low Risk' categories according to risk perceived based on PFSPL's experience, and assessment and they will be reviewed at least Once in a year.

- Risk categorization will be undertaken based on parameters such as
    - Loan Amount
    - Client Annual Income
    - Client Loan Cycle
    - Geographical risks
    - Types of transaction
    - Major Income Source

While considering the customer's identity, the ability to confirm identity documents online or other services offered by issuing authorities will also be factored in.

- PFSPL will devise procedures for creating risk profiles of its existing and new customers and apply various Anti-Money Laundering measures keeping in view the risks involved in a financial transaction. The due diligence and monitoring will be aligned with the risk category of customers.

- PFSPL's internal audit and compliance functions will play an important role in evaluating and ensuring adherence to KYC policies and procedures, including legal and regulatory requirements. The staff will, at all points of time, be trained adequately and will be well versed in such policies and procedures at all the Branches.

The criteria for client risk categorization are given below:

Criteria	Range	Risk Rating
Loan Amount	< 1 Lac	0
	>1 Lac < 10 Lacs	1
	>10 Lacs	2
Client Annual Income	1 - 3 Lacs / Year	0
	3 - 6 Lacs / Year	1
	>6 or <1 Lacs Per Year	2
Client Loan Cycle	Beyond 6th Cycle	0
	3rd To 6th	1
	1st To 2nd	2
Location Geographical Risk	Low-Risk Zone	0
	Mid-Risk Zone	1
	High-Risk Zone	2
Types Of Transactions Undertaken	Digital	0
	Cash	1
Major Income Source	Salaried	0
	Business	1
	Part-Time	2

Risk Category	Total Risk Rating	Frequency of Review
High	11-8	Every 2 years
Medium	7-4	Every 8 Years
Low	3-0	Every 10 years

High-risk accounts will be subjected to more intensified monitoring. A system of periodic review of risk categorization of such accounts, with such periodicity being at least once every year and the need for applying enhanced due diligence measures will be put in place as mentioned in the RBI KYC Master Direction 2016- - Enhanced and Simplified Due Diligence Procedure (amended from time to time)
KYC updation in line with the risk categorization framework will be undertaken.

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.

6.3 Customer Identification Procedure (CIP)

Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data, or information. Branches need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or

occasional and the purpose of the intended nature of the financial relationship. Being satisfied means that the branch must be able to satisfy the authorities that due diligence was observed based on the risk profile of the customer in compliance with the guidelines in place. Branches should obtain sufficient identification data, such as the address/location and recent photograph, to verify the identity of the customer.

PFSPL shall undertake the identification of the customers in the following cases:

i. Commencement of an account-based relationship with the customer.
ii. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

PFSPL may collect such documents and other information in respect of different categories of its customers depending on perceived risk and keeping in mind the requirements of the Prevention of Money Laundering Act, 2002, and guidelines issued by the RBI from time to time. Besides risk perception, the nature of information/documents required would also depend on the type of customer.

While preparing the customer profiles, PFSPL would take care to seek only such information from the customer that is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein shall not be divulged for cross-selling or any other purposes, unless consented to, in writing, by the concerned customer.

7 Customer Due Diligence (CDD)

Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable.

- Taking reasonable steps to understand the nature of the customer's business, and its ownership and control.
- Determining whether a customer is acting on behalf of a beneficial owner, identifying the beneficial owner, and taking all steps to verify the beneficial owner's identity, using reliable and independent sources of identification.

8 Other Guidelines

- PFSPL will not form any relationship with shell banks.
- PFSPL will only operate with correspondent banks that have the license to operate in their country of origin.
- PFSPL will not establish any relationship with unlicensed banks or NBFCs.

9 Internal Audit

PFSPL's internal audit department will evaluate and ensure adherence to the KYC policies and procedures. As a rule, the compliance function will provide an independent evaluation of PFSPL's policies and procedures, including legal and regulatory requirements. Internal Auditors may specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this

regard. Compliance in this regard will be put up before the Audit Committee of the Board along with their normal reporting frequency.

The internal audit procedures will be periodically tested and evaluated for their effectiveness. Based on the evaluation, it will be revised at regular intervals.

10 Non-cooperation by the customer concerning KYC norms.

Where PFSPL is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, PFSPL will follow up with the existing identified customers for KYC compliance, Closure decision if at all required will depend upon our internal assessment and will be taken at a Senior Level of State Heads and above only after issuing due notice to the customer explaining the reasons for taking such a decision.

11 Combating Financing of Terrorism (CFT)

To ensure that criminals are not allowed to misuse the banking/financial channels, PFSPL will put up adequate screening mechanisms not only in respect of customers and vendors but also in matters of recruitment and hiring of personnel.

Towards the purpose, PFSPL will refer to the list of individuals and entities circulated by RBI, approved by the Security Council Committee established under various United Nations Security Council Resolutions (UNSCRs), as and when received from the Government of India.

PFSPL would ensure to update the consolidated list of individuals and entities as circulated by RBI and before opening any new account would ensure that the name/s of the proposed customer does not appear on the list.

Further, PFSPL would scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list would immediately be intimated to RBI and FIU-IND by the Principal Officer of PFSPL.

11.1 Money Laundering and Terrorist Financing Risk Assessment

- PFSPL will carry out the 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess, and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The assessment process will consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, PFSPL will take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share from time to time.

- The risk assessment will be proportionate to PFSPL's nature, size, geographical presence, complexity of activities/structure, etc. It will be properly documented. Further, the periodicity of the risk assessment exercise shall be determined in alignment with the outcome of the risk assessment exercise. It will be reviewed annually.
- The outcome of the exercise will be put up with the Board or any committee of the Board to which power in this regard has been delegated and will be available to competent authorities and self-regulating bodies.
- PFSPL shall apply a Risk-Based Approach (RBA) for the mitigation and management of risks and will have Board approved policies, controls, and procedures in this regard. PFSPL will implement a CDD program, having regard to the ML/TF risks identified and the size of the business. Further, PFSPL will monitor the implementation of the controls and enhance them if necessary.

12 Information to be preserved (Record Management)

PFSPL will take the following steps regarding maintenance, preservation, and reporting of customer account information, regarding the provisions of the PML Act and Rules. PFSPL will:

a) Maintain all necessary records of transactions between PFSPL and the customer for at least five years from the date of the transaction.
b) Preserve the records of the identification of the customers and their addresses obtained while opening the account and during the business relationship, for at least five years after the business relationship is ended.
c) make available the identification records and transaction data to the competent authorities upon request.
d) PFSPL will make available identification records and transaction data to the competent authority upon request. For this, a proper system will be evolved 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.
e) maintain records of the identity and address of the customer, and records in respect of transactions referred to in PML Rule 3 in hard or soft format.

13 Reporting to Financial Intelligence Unit-India

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 format as available on the FIU India Portal.

The Principal Officer will record reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office.

Cash Transaction Reports (CTR)

- Identify cash transactions ≥ ₹10,00,000 (single or series).
- File CTR to **FIU-IND** by the **15th of the next month**.
- Maintain an audit trail for reported CTRs.

Suspicious Transaction Reports (STR)

- Detect and analyse suspicious transactions (in nature or value). The Company shall endeavor to put in place automated systems for monitoring transactions to identify potentially suspicious activity.
- File STR within **7 days of forming suspicion** to FIU-IND.
- STR filing will be kept confidential, so that there is no tipping off to the customer.

14. Requirements/obligations under International Agreements

14.1 Communications from International Agencies –

PFSPL will ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, it does not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the lists are as under:

a) The **"ISIL (Da'esh) &Al-Qaida Sanctions List"**, which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL &Al-Qaida Sanctions List is available at https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl

b) The **"1988 Sanctions List"**, consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl.

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising the Ministry of Home Affairs.

PFSPL will regularly check its partners, sub-partners, or contractors against these lists.

In addition to the above, other UNSCRs circulated by the Reserve Bank of India in respect of any other jurisdictions/ entities from time to time shall also be taken note of.

In addition to the above, a process/procedure will be put in place process (as and when required) to regularly check PFSPL partners, sub-partners, or contractors against the lists shared/required by PFSPL lending partners/any other jurisdictions/entities from time to time.

14.2 Secrecy Obligations and Sharing of Information

a) PFSPL will maintain secrecy regarding the customer information which arises out of the contractual relationship between PFSPL and the customer.

b) Information collected from customers for opening of account will be treated as confidential and details thereof shall not be divulged for cross-selling, or any other purpose without the express permission of the customer.

c) While considering the requests for data/information from the Government and other agencies, PFSPL will satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.

d) The exceptions to the said rule shall be as under:
   - Where disclosure is under compulsion of law
   - Where there is a duty to the public to disclose,
   - the interest of PFSPL requires disclosure and

- Where the disclosure is made with the express or implied consent of the customer.
- PFSPL shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

15 Hiring of Employee and Employee Training

PFSPL will put in place adequate screening mechanisms including Know Your Employee as an integral part of their personnel recruitment/hiring process.

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

PFSPL will have an ongoing employee training program so that the members of staff are adequately trained in AML/CFT policy. The focus of the training will be different for frontline staff, compliance staff, and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from a lack of customer education. Proper staffing of the audit function with people adequately trained and well-versed in AML/CFT policies of PFSPL, regulation, and related issues will be ensured.

16 Customer Education

PFSPL will educate the customer on the objectives of the KYC program so that the customer understands and appreciates the motive and purpose of collecting such information.

17 Introduction of New Technologies

PFSPL will pay special attention to any money laundering threats that may arise from new or developing technologies including online transactions that may favor anonymity, and take measures, if needed, to prevent their use in money laundering schemes as and when online transactions are started /accepted by PFSPL.

PFSPL shall identify and assess the ML/TF risks that may arise about the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Further, PFSPL shall ensure:

(a) to undertake the ML/TF risk assessments before the launch or use of such products, practices, services, technologies; and

(b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

18. Annexure

Annexure - A

PFSPL will obtain any one of the certified copies of an "Officially Valid Document" (OVD) from an individual while establishing an account-based relationship. OVD means:

- Passport
- Driving license
- Proof of possession of Aadhaar number
- 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
- 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 the Aadhaar number as an OVD, he may submit it in such form as issued by the Unique Identification Authority of India.

b. Where the OVD furnished by the customer does not have an updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address: -

   i. Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

   ii. property or Municipal tax receipt.

   iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address.

   iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions, and listed companies and leave and license agreements with such employers allotting official accommodation.

- One Recent Passport photograph
- The Permanent Account Number or Form No. 60 as defined in Income-tax Rules, 1962
- Any other such document is required in addition to the above-mentioned documents about the nature and business requirements of PFSPL.

PAHAL
A NEW BEGINNING

Annexure – B

List of Suspicious Activities / Transactions:

1. An employee whose lavish lifestyle cannot be supported by his or her salary.
2. Negligence of employees/willful blindness is reported repeatedly.
3. Large Cash Transactions reported in existing / new customers.
4. Multiple accounts under the same name of the customers.
5. Sudden surge in activity level in customer(s) account.
6. The same funds are being moved repeatedly among several accounts of the customer(s).

****