

PAHAL FINANCIAL SERVICES PRIVATE LIMITED

Know Your Customer (KYC) and Anti Money Laundering (AML) Policy

Name	Designation	Signature	Date
Mr. Kartik S Mehta	Managing Director		
Ms. Purvi J Bhavsar	Managing Director		
Mr Deepak Billa	Head – Audit & Risk		

The Know Your Customer (KYC) and Anti Money Laundering (AML) Policy is approved by the Board of Directors at the Board Meeting held on 14th April 2020

Prepared by

Name	Designation	Signature	Date
Ms. Nikita Sharma	Company Secretary		

Registered Office: First Floor-2, City Mall, Nr. Rajpath Club, Opp. Madhur Hotel S.G Highway,
Bodakdev, Ahmedabad – 380059

Phone No.: 079-40373857

Email Id: ho@PFSPfinance.com

Table of Contents

1	Preamble	3
2	Objectives.....	3
3	Applicability.....	3
4	Definitions	3
5	Designated Authorities	4
5.1	Designated Director	4
5.2	Principal Officer.....	5
6	Policy	5
6.1	Customer Acceptance Policy (CAP)	5
6.2	Risk Management	6
6.3	Customer Identification Procedure (CIP)	7
7	Internal Audit	8
8	Non-Cooperation by the customer in respect of KYC norms.....	8
9	Combating Financing of Terrorism (CFT)	8
9.1	Money Laundering and Terrorist Financing Risk Assessment	9
10	Information to be preserved (Record Management)	9
11	Reporting to Financial Intelligence Unit-India	10
12	Requirements/obligations under International Agreements	10
12.1	Communications from International Agencies –	10
12.2	Secrecy Obligations and Sharing of Information	11
13	Hiring of Employee and Employee Training.....	11
14	Customer Education.....	11
15	Introduction of New Technologies.....	11
16	Annexure	13

1 Preamble

As a Non-banking Finance Company-Microfinance Institution (NBFC-MFI), registered with the Reserve Bank of India (RBI), PF SPL Financial Services Pvt. Ltd. (PF SPL) 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 to the prevalent KYC Policy, duly edited in line with the latest guidelines of Reserve Bank of India.

The policy will be in compliance 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 on April 20, 2020) 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 PF SPL from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable PF SPL to know/understand customers and their financial dealings better which in turn help 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 safeguarding PF SPL from being unwittingly used as conduit for transfer or deposit of funds derived from criminal activity or for financing of 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 is applicable to each and every business activity of PF SPL. Any contravention or non-compliance will attract 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 PF SPL.

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 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
- **Designated Director-** A person designated by PFSP to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules.
- **Principal Officer-** An officer nominated by the RE, responsible for furnishing information as per rule 8 of the Rules.
- **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. 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
 - ii. appears to be made in circumstances of unusual or unjustified complexity
 - iii. appears to not have economic rationale or bona-fide purpose
 - iv. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
- **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.
- **Certified Copy:** Obtaining a certified copy by PFSP shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of PFSP as per the provisions contained in the Act.

5 Designated Authorities

5.1 Designated Director

“Designated Director” will be designated by PFSP 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	
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	Mr Deepak Billa
Designation	Head – Audit & Risk
Phone	+917228930171
Email	deepak.billa@pahalfinance.com

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

Managing Director (MD) of PFSPL will take necessary steps to advise the concerned staff about the importance of compliance with above KYC & PMLA norms.

6 Policy

The KYC policy includes 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 acceptance of customers. The Customer Acceptance Policy shall ensure that explicit guidelines are in place on the following aspects of customer relationship in PFSPL.

1. No account is opened in 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, so as to ensure that the identity of the customer on the basis of 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 purpose 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. PFSP will apply the CDD procedure at the Unique Customer Identification Code (UCIC) level. Thus, if an existing KYC compliant customer of PFSP desires to open another account with the PFSP, 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 clearly spelt out.
8. 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 sanctions lists circulated by Reserve Bank of India.
9. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

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

6.2 Risk Management

PFSP will apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and have policies, controls, and procedures in this regard. Further, PFSP 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 its experience, assessment and review it from time to time.

Risk categorization will be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, Loan amount and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities will also be factored in.

PFSP 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.

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

The criteria for client risk categorization is given below:

Criteria	Range	Risk Rating	Range	Risk Rating	Range	Risk Rating
Loan Amount	< 1 Lac	0	>1 lac < 10 lacs	1	>10 Lacs	2
Client Annual Income	< 5 Lacs / year	0	5 – 10 Lacs / year	1	>10 lacs per year	2

Client Loan Cycle	1 st to 2 nd	2	3 rd to 6 th	1	Beyond 6 th cycle	0
-------------------	------------------------------------	---	------------------------------------	---	------------------------------	---

Risk Category	Total Risk rating	Frequency of review
High	6-5	Every 2 year
Medium	4-2	Every 5 Year
Low	1-0	Every 10 years

High risk accounts will be subjected to more intensified monitoring. A system of periodic review of risk categorisation 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.

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 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.

PFSP 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.

PFSP shall ensure that decision-making functions of determining compliance with KYC norms will not be outsourced.

PFSP 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 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 the customer.

PFSP will categorize the profile for each new customer based on risk categorization. The customer profile may contain information relating to customer's identity, profile, social / financial status and nature and location of its business activity. The nature and extent of due diligence will depend on the risk categorization as defined in this policy. However, while preparing customer profile, PFSP would take care to seek only such information from the customer which 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 Internal Audit

PFSP's internal audit department will evaluate and ensure adherence to the KYC policies and procedures. As a general rule, the compliance function will provide an independent evaluation of PFSP's own 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. The 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 tested at least annually and evaluated for its effectiveness. Based on the evaluation, it will be revised at regular intervals.

8 Non-Cooperation by the customer in respect of KYC norms

Where PFSP is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, PFSP will follow up with the existing identified customers for KYC compliance, Closure decision if at all is 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.

9 Combating Financing of Terrorism (CFT)

In order to ensure that criminals are not allowed misusing the banking/financial channels, PFSP will put up adequate screening mechanism not only in respect of customers and vendors but also in matters of recruitment and hiring of personnel.

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

PFSP 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 in the list.

Further, PFSP 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 PFSP.

Similar caution will be exercised while dealing with clients originating from countries having deficient AML / CFT Standards as per FATF.

9.1 Money Laundering and Terrorist Financing Risk Assessment

- PFSP will carry out '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, PFSP 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 PFSP's nature, size, geographical presence, complexity of activities/structure, etc. It will be properly documented. Further, the periodicity of 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 to 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

10 Information to be preserved (Record Management)

PFSP will take following steps regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. PFSP will:

- a) Maintain all necessary records of transactions between PFSP 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 while opening the account and during 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) PFSP 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.

11 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 formats at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat, Chanakyapuri, New Delhi-110 021

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.

12 Requirements/obligations under International Agreements

12.1 Communications from International Agencies –

PFSP 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 Ministry of Home Affairs as required under UAPA notification dated March 14, 2019.

PFSP 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 checks PFSP partners, sub-partners or contractors against the lists shared/required by PFSP lending partners/any other jurisdictions/entities from time to time.

12.2 Secrecy Obligations and Sharing of Information

- a) PFSP will maintain secrecy regarding the customer information which arises out of the contractual relationship between PFSP and customer.
- b) Information collected from customers for the purpose of opening of account will 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, PFSP 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:
 - a. Where disclosure is under compulsion of law
 - b. Where there is a duty to the public to disclose,
 - c. the interest of PFSP requires disclosure and
 - d. Where the disclosure is made with the express or implied consent of the customer.
- e) PFSP shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

13 Hiring of Employee and Employee Training

PFSP will put in place adequate screening mechanism as an integral part of their personnel recruitment/hiring process.

PFSP will have an on-going employee training programme 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 lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of PFSP, regulation and related issues will be ensured.

14 Customer Education

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

15 Introduction of New Technologies

PFSP will pay special attention to any money laundering threats that may arise from new or developing technologies including on-line 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 PFSP.



PAHAL
A NEW BEGINNING

16 Annexure

Annexure - A

PFSP will obtain any one of the certified copy of “Officially Valid Document” (OVD) from an individual while establishing an account based relationship. OVD means:

- Valid Passport
- Valid 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 Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
 - b. Where the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:-
 - i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
 - ii. property or Municipal tax receipt;
 - iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
 - iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;
- the customer shall submit OVD with current address within a period of three months of submitting the documents specified above
 - One Recent Passport photograph
 - If required, The Permanent Account Number or Form No. 60 as defined in Income-tax Rules, 1962
 - Any other such document required in addition to above mentioned documents pertaining to the nature and business requirement of PFSP.

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. Same funds being moved repeatedly among several accounts of the customer(s).
