SAVE

Inclusion-Growth-Prosperity

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

of

Save Microfinance Private Limited

Inclusion-Growth-Prosperity

1. PREAMBLE:

The Reserve Bank of India (RBI) has issued comprehensive 'Know Your Customer' (KYC) Guidelines to all Non-Banking Financial Companies (NBFCs)-MFI in the context of the recommendations made by the Financial Action Task Force (FATF) and Anti Money Laundering (AML) standards and Combating Financing of Terrorism (CFT) policies, as these being used as the International Benchmark for framing the stated policies, by the regulatory authorities.

In view of the same, Save Microfinance Private Limited ("SMPL" or "the Company") has adopted the said KYC guidelines with suitable modifications depending on the activity undertaken by it. The Company has ensured that a proper policy framework on KYC and AML measures be formulated in line with the prescribed RBI guidelines and put in places duly approved by its Board of Directors.

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 May 10, 2021) or any subsequent change in the notification/master direction

The Policy will fall due for review yearly.

2. OBJECTIVES, SCOPE AND APPLICATION OF THE POLICY:

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

1. To prevent criminal elements from using Save Microfinance Private Limited for money laundering activities.
2. To enable Save Microfinance Private Limited to know/ understand its customers and their financial dealings better which, in turn, would help the Company to manage risks prudently.
3. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
4. To comply with applicable laws and regulatory guidelines.
5. To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures.

3. APPLICABILTIY

This KYC Policy is applicable to all offices (if any) of Save Microfinance Private Limited and is to be read in conjunction with related operational guidelines issued from time to time. This Policy includes some key elements:

1. Customer Acceptance Policy (CAP)

2. Customer Identification Procedures (CIP)
3. Monitoring of Transactions
4. Risk management
5. Training Programme
6. Internal Control Systems

4. DEFINITIONS

- **Customer-** A Customer is defined as a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
- **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 the Company 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 Company, 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 the Company shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or Officially Valid Document(s) so produced by the customer with the original and recording the same on the copy by the authorised officer of SMPL as per the provisions contained in the Act.
- **Officially Valid Document** (OVD) means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

5. IMPLEMENTATION OF THIS POLICY

Mr. Pankaj Kumar, Director of the Company act as the Designated Director of the Company and who will be responsible for:

- Compliance of the provisions of the PMLA and AML Guidelines.
- Act as a central reference point and play an active role in Identification & assessment of potentially suspicious transactions.
- Ensure that SMPL discharges its legal obligation to report suspicious transactions to the concerned authorities.

Mr. Ajeet Kumar Singh, Director of the Company act as the Principal Officer of the Company and who will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. The Principal Officer will report the same to the Board/Audit Committee, if any.

The main aspect of this policy is the Customer Due Diligence Process which means:

- Obtaining sufficient information about the client in order to identify who is the actual borrower of the loan or on whose behalf transaction is conducted.
- Verify the customer's identity using reliable, independent source document, data or information.
- Conduct on-going due diligence and scrutiny of the documents/client to ensure that the transaction conducted are consistent with the client's background/financial status, its activities and risk profile.

5.4 Customer Due Diligence

The Customer Due Diligence Process includes four specific parameters:

5.4.A Customer Acceptance Policy (CAP)
5.4.B Client Identification Procedure (CIP)
5.4.C Suspicious Transactions identification & reporting
5.4.D Monitoring of Transactions

5.4.A Customer Acceptance Policy (CAP)

SMPL 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 SMPL.

- ***Each client should be met in person***: Accept client whom we are able to meet personally. We should meet the client at his residence address to get the necessary documents filed in and signed. Preferably accept clients who live within the jurisdiction of the branch. As far as possible, ensure

that the new client reference check is done and credit bureau check and details is obtained pre-funding.

- ***Accepts clients on whom we are able to apply appropriate KYC procedures:*** Obtain complete information from the client. It should be ensured that the initial forms taken by the clients are filled in completely. All photocopies submitted by the client are checked against original documents without any exception. Ensure that the 'Know Your Client' guidelines are followed without any exception. All supporting documents as specified by RBI are obtained and verified.
- ***Do not accept clients with identity matching persons known to have criminal background***: Check whether the client's identify matches with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement/regulatory agency worldwide.
- ***Be careful while accepting Clients of Special category***: We should be careful while accepting clients of special category like Politically Exposed Persons (PEP) and their family members, non-face to face clients, clients with dubious background. Scrutinize minutely the records/documents pertaining to clients belonging to aforesaid category.
- ***Do not compromise on submission of mandatory information/documents:*** Customer should be lent only on receipt of mandatory information along with authentic supporting documents as per the regulatory guidelines. Do not lend where the customer refuses to provide information/ documents and we should have sufficient reason to reject the customer towards this reluctance. 'Optional'/additional information is obtained with the explicit consent of the customer after the account is opened.

5.4.A.ii Policy for acceptance of clients:

The Company would develop customer acceptance policies and procedures that aim to identify the types of customers that are likely to pose a higher than the average risk of money laundering or terrorist financing. By establishing such policies and procedures, they will be in a better position to apply customer due diligence on a risk sensitive basis depending on the type of customer business relationship or transaction. In a nutshell, the following safeguards would be followed while accepting the clients:

a) No account is opened in a fictitious / benami name or on an anonymous basis.

b) Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to clients' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. The parameters should enable classification of clients into low, medium and high risk. Clients of special category (as given below) may, if necessary, be classified even higher. Such clients require higher degree of due diligence and regular update of KYC profile.

c) Documentation requirement and other information to be collected in respect of different classes of clients depending on perceived risk and having regard to the requirement to the Prevention of Money Laundering Act 2002, guidelines issued by RBI and SEBI from time to time.

d) Ensure that an account is not opened where the Company is unable to apply appropriate clients due diligence measures / KYC policies. This may be applicable in cases where it is not possible to ascertain the identity of the client, information provided to the intermediary is suspected to be non-genuine, perceived non- cooperation of the client in providing full and complete information. The market intermediary should not continue to do business with such a person

and file a suspicious activity report. It should also evaluate whether there is suspicious trading in determining in whether to freeze or close the account. The market intermediary should be cautious to ensure that it does not return securities of money that may be from suspicious trades. However, the market intermediary should consult the relevant authorities in determining what action it should take when it suspects suspicious trading.

e) The circumstances under which the client is permitted to act on behalf of another person / entity should be clearly laid down. It should be specified in what manner the account should be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity / value and other appropriate details. Further the rights and responsibilities of both the persons (i.e. the agent- client registered with the intermediary, as well as the person on whose behalf the agent is acting should be clearly laid down). Adequate verification of a person's authority to act on behalf the customer should also be carried out.

f) Necessary checks and balance to be put into place before opening an account so as to ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide.

g) The Company will apply the CDD procedure at the Unique Customer Identification Code (UCIC) level. Thus, if an existing KYC compliant customer of the Company desires to open another account with the Company, there shall be no need for a fresh CDD exercise.

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

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

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

5.4.A.iii Risk-based Approach

It is generally recognized that certain customers may be of a higher or lower risk category depending on circumstances such as the customer's background, type of business relationship or transaction etc. As such, the Company would apply each of the customer due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that the Company would adopt an enhanced customer due diligence process for higher risk categories of customers. Conversely, a simplified customer due diligence process may be adopted for lower risk categories of customers. In line with the risk-based approach, the type and amount of identification information and documents that the Company would obtain necessarily depend on the risk category of a particular customer.

5.4.B Customer Identification Procedure & KYC (For New/Old/Existing Customer) Individuals Only

Objective: To have a mechanism in place to establish identity of the customer along with firm proof of address & Identity to prevent giving /lending loan which is fictitious / benami / anonymous in nature.

5.4.B.i. Documents which can be relied upon:

- **IDENTITY PROOF**: Voter Card is mandatory and is most reliable document as only once card is issued to an individual and we can independently check its genuineness through Election Commission web site. However, in case voter card carries an old photograph, which does not match current facial features of the client, we should take other identity proof in form of proof of possession of Aadhaar Card Issued by UIDAI (in case, where offline verification cannot be carried out), Valid Passport, Valid Driving License, ID card issued by Central / State Government, 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.

- **ADDRESS PROOF:** For valid address proof we can rely on Voter's Identity Card, proof of possession of Aadhaar Card Issued by UIDAI (in case, where offline verification cannot be carried out), Valid Passport, Ration Card, , Valid Driving License, ID card issued by Central / State Government with address mentioned in it, State and Central government department utility bills not older than 60 days from the billing date, Bank passbook with photograph, land title, Property Tax receipt with address mentioned in it.

- **AGE PROOF:** For genuine age we can rely on Voter's Identity Card, proof of possession of Aadhaar Card Issued by UIDAI (in case, where offline verification cannot be carried out), Valid Passport, Ration Card, PAN Card, Valid Driving License, Identity card issued by Central / State Government with date of birth mentioned in it, Birth Certificate issued by local municipal corporation.

  Detailed documents for KYC are mentioned in 'Annexure A - Officially Valid Documents'

5.4.B.ii. General Guidelines

- Always check original documents before accepting the copies.
- Obtain the latest photograph of borrower / guarantor / spouse.
- Review the above details on, on-going basis to ensure that the transactions being conducted are consistent with our knowledge of customers, its business and risk profile, taking into account, where necessary, the customer's source of funds.
- Scrutinize the forms submitted by the customer thoroughly and cross check the details with various documents submitted by the customer.
- Should be referred also and RBI Defaulters Database available on http://www.cibil.com/ can be checked.
- Employee of SMPL should not sign as witness on any sort of form.

5.4.B.iii. Risk Profiling of the Clients

SMPL 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, SMPL will monitor the implementation of the controls and enhance them if necessary.

We should accept the customer's based on the risk they are likely to pose. The aim is to identify customers who are likely to pose a higher-than-average risk of money laundering or terrorist financing. For this purpose, we need to classify the clients as Low risk and high-risk clients. By classifying the clients, we will be in a better position to apply appropriate customer due diligence process. That is, for high-risk customer we have to apply higher degree of due diligence. The factors

of risk perception depend on customer's location, nature of income activity, nature of transaction, manner of payment 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.

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.

SMPL 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.

The criteria for client risk categorization is given below:

Criteria	Range	Risk Rating	Range	Risk Rating	Range	Risk Rating
Loan Amount	< 50K	0	>50 lac < 1 lacs	1	>1 Lacs	2
Client Annual Income	< 3 Lacs / year	0	3 – 5 Lacs / year	1	>5 lacs per year	2
Client Loan Cycle	1st to 2nd	2	3rd to 6th	1	Beyond 6th cycle	0

Risk Category	Total Risk rating	Frequency of review
High	6-5	Every 2 year
Medium	4-3	Every 8 Year
Low	2-0	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. Periodic updation of the KYC will be carried out as per the Risk Category of the client from the date of opening of the account / last KYC updation.

No change in KYC information: In case of no change in the KYC information, a self-declaration from the customer in this regard will be obtained through customer's email-id registered with the Company, customer's mobile number registered with the RE, digital channels, 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 email-id registered with the Company, customer's mobile number registered with the Company, digital channels, letter etc., and the

declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

Further, the Company, at its option, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of address, declared by the customer at the time of periodic updation.

For periodic updation, a recent photograph, physical presence of the customer is required. Periodic updation of KYC can only be carried out in the branch of the Company where account is maintained by the customer.

Any change in the risk profile of the customer has to be ascertained by the concerned branch officials and reported to the Business Head immediately.

SMPL'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.

5.4.B.iv. ROLES

a. Customer Relationship Officer / Branch Manager/ Area Manager / Regional Manager / State Head:

- The CRO/Sr.CRO/BM/Sr.BM should meet the customer in person at least once before approving/ disbursing loan at the address given by the customer. In the process he may reasonably verify the living standards, source of income, financial / social status, etc. of the customer and ensure that the details mentioned in the digital CRF (Customer Registration Form) matches with the actual status.
- If the customer is a 'walk-in customer', then the concerned branch official should make independent verification about the background, identity and financial worthiness of the customer.
- All mandatory proofs of identity, address and financial status of the customer must be collected as prescribed by the regulatory authorities, from time to time. The proofs so collected should be verified with the originals. If the prospective customer is refusing to provide any information do not forward his/ her loan application form to HO.
- The Branch Manager/ Senior Branch Manager has to be completely satisfied about the background, genuineness and financial / social status of the customer before recommending/Approving / disbursing loan. If required, the Branch Manager may seek additional information/documents from the customer.

b. **Risk & Audit Management Team**

Risk and Audit Management Team (RAMT) visit the customer individually and in group as and when required to in place of and verify the details obtained verbally/documentary, gives report to Risk & Audit Head on customer/staff based on the information available from the market source/ documentary source and interaction with the different customer/groups.

Activity of the customer, which is not commensurate with the financial /social details, declared by the customer/group, it should be analyzed and referred to the Principal Officer with reasons of suspicion.

c. **Role of Human Resource Department**

- The Human Resource Department and other Department Heads involved in hiring new employees should have adequate screening procedure in place to ensure high standards in hiring new employees.
- Bona fides of employees are checked to ensure that the employees do not have any link with terrorist or other anti-social organizations.
- Not only Know Your Customer (KYC) policy but also "Know Your Employee" procedures should be in place.
- Briefings to new employees at induction programs and rounds of small meetings and presentations at branch locations.
- Adequate training should be given to all the concerned employees to (a) ensure that the contents of the guidelines are understood and (b) develop awareness and vigilance to guard against money laundering and terrorist financing.
- As of now, SMPL AML policy will be covered during the induction training given to all new recruits and also during the on-going compliance sessions at the regions.

d. Role of Area Manager / Regional Managers / State Heads /Zonal Heads

- Being in the field, they have market intelligence about potential mischief makers which should be brought to the notice of RAMT.
- KYC forms and other documents drafted should invariably have undertaking from the customer that he is not indulging in or has not been associated with any money-laundering activity or terrorist activity and that he has not been convicted of any fraud/offence/ crime by any regulatory authority existing in the country.
- All disclosure documents should have notice to the customer informing about company's right to obtain and disclose any information about the customer to the competent authority as may be required.

5.4.C. Suspicious Transactions

All are requested to analyze and furnish details of suspicious transactions, whether or not made in cash. It should be ensured that there is no undue delay in analysis and arriving at a conclusion.

5.4.C.i. What is a Suspicious Transaction: Suspicious transaction means a transaction whether or not made in cash, which to a person acting in good faith:

- Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or

- Appears to be made in circumstance of unusual or unjustified complexity; or
- Appears to have no economic rationale or bona fide purpose.

Reasons for Suspicious:

- Identity of customer
  - False identification documents
  - Identification documents which could not be verified within reasonable time
  - Non-face to face customer
  - Customers in high-risk jurisdiction
  - Doubt over the real beneficiary of the loan
- Suspicious Background
  - Suspicious background or links with criminals
- Nature of Transactions
  - Unusual or unjustified complexity
  - No economic rationale or bonafide purpose
  - Source of fund are doubtful
  - Transactions reflect likely market manipulations

5.4.C.ii. When to Report

In terms of the PMLA rules, Principal Officer is required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU- IND) at 6th Floor, Hotel Samarat, Chanakyapuri, New Delhi - 110021 as per the schedule given below:

Report	Description	Due Date
CTR	All cash transactions of the value of more than Rs.10 Lakhs or its equivalent in foreign Currency	NOT APPLICABLE TO NBFCs-MFI AS OF NOW
	All series of cash transactions Integrally connected to each other which have been valued below Rs. 10 Lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month	NOT APPLICABLE TO NBFCs-MFI AS OF NOW
CCR	All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions*	Upto fifteen days of the succeeding month.
	All suspicious transactions whether or not made in cash	Upto fifteen days of the succeeding month.

NTR	Non-Profit Organization Transaction Report	NOT APPLICABLE O NBFCs-MFI AS OF NOW

5.4.C.iii. Combating Financing of Terrorism (CFT)

To ensure that criminals are not allowed misusing the banking/financial channels, SMPL 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, SMPL 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.

SMPL 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, SMPL 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 SMPL.

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

5.4.C.iv. Money Laundering and Terrorist Financing Risk Assessment

- SMPL 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, SMPL 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 SMPL'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.

In view of the same, Area Manager /Regional Managers / State Heads / Zonal Head are required to collect information from the Branches/Departments/Customers/Group under their control/ jurisdiction and submit report on suspicious transactions Risk & Audit head. Risk & Audit Head will submit the details to the Principal Officer within 15 working days of establishment of such transaction to enable the Principal Officer to report the same to the Director, Financial Intelligence Unit-India (FIU-IND) within the stipulated time.

5.4.C.v. Other Important Points

- Reasons for treating any transaction or a series of transactions as suspicious should be recorded. It should be ensured that there is no undue delay in arriving at such a conclusion.
- Utmost confidentiality should be maintained in submitting the information.
- The reports may be transmitted by email/speed/registered post/fax at the Head Office addressed to the Principal Officer.
- No restriction may be put in the client account, where a Suspicious Transaction found / noticed.
- It should be ensured that there is no tipping off to the client at any level.

5.4.D. Monitoring of Transactions

SMPL would continue to maintain proper record of all cash transactions of INR l0 Lakhs and above and have in place centralized internal monitoring system at head office.

SMPL would strive to have an understanding of the normal and reasonable activity of the clients through personal visits and by observing the transactions and conduct of the account in order to identify transactions that fall outside the regular pattern of the activity - unusual transactions.

The following transactions would be considered as unusual transactions deserving special attention. unusual transactions by the Principal Officer - PMLA.

- Repeated pre-termination of the loan accounts of size exceeding INR I0 lakhs;
- Same client appearing in the Cash Transaction Report (CTR) more than 3 times during a span of 6 months;
- Total cash received from a client in a financial year exceeding INR 50 lakhs.
- SMPL is not empowered to seize any counterfeit currency. However, the following incidents of counterfeit currency at the cash counter would be recorded and repeated occurrence would be reported.
- Bulk counterfeit currency of more than 10 pieces at a time;
- Repeated event within a week from a collection executive or client.

All CTR/STR would be filed electronically or as per the norms stipulated by FIU-IND from time to time. The STR would be filed for even for attempted transactions.

6. Formulate/Review/Training on the Internal Policy & Procedure to All Employees

- This internal policy and procedure on “The Prevention of Money Laundering Act, 2002” should be brought to the notice of all employees by Human Resource Department through the Company’s intranet.
- Staff training and implementing specific procedures for customer identification and retaining internal records of transactions.
- The Internal Policy should be placed before the Business Head and if any changes in the policy are warranted, the revised policy should be placed before the Board for review and approval.

7. Record Keeping Requirements

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

a)Maintain all necessary records of transactions between SMPL 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)SMPL 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.

8. Requirements/obligations under International Agreements

Communications from International Agencies

SMPL 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 February 2, 2021.

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

Secrecy Obligations and Sharing of Information

a) SMPL will maintain secrecy regarding the customer information which arises out of the contractual relationship between SMPL 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, SMPL 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 SMPL requires disclosure and
    d. Where the disclosure is made with the express or implied consent of the customer.
e) SMPL shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

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

(a) Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

(b) In terms of provision of Rule 9(1A) of PML Rules, the Company will capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

(c) Operational Guidelines released by CERSAI will be taken into account while uploading the KYC data.

(d) SMPL will capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates if revised, from time to time, as may be required and released by CERSAI, will be updated by SMPL.

(g) Once KYC Identifier is generated by CKYCR, SMPL would ensure that the same is communicated to the customer.

(h) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, SMPL would upload/ update the KYC data pertaining to accounts of individual customers opened prior to the April 1, 2017, at the time of periodic updation, or earlier, when the updated KYC information is obtained/received from the customer.

(i) SMPL would ensure that during periodic updation, the customers are migrated to the current CDD standard.

(j) Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to the Company, with an explicit consent to download records from CKYCR, then SMPL will retrieve the KYC records online from the CKYCR using the KYC Identifier and the customer will 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.

10. DESIGNATED DIRECTOR

The Board of Directors of the Company has nominated Mr. Pankaj Kumar, Director of the Company as "Designated Director" as required under provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, to ensure compliance with the obligations under the Act and Rules. In case any further information /clarification is required in this regard, the 'Designated Director' may be contacted as per details mentioned below:-

Mr. Pankaj Kumar, Director

SAVE MICROFINANCE PRIVATE LIMITED
"Head office"
SAVE Tower, Asha Singh More,
A.P. Colony, Gaya – 823001, Bihar Tel: 011-61325102
Email: director1@saveind.in

11. PRINCIPAL OFFICER

Mr. Ajeet Kumar Singh, Director of the Company is designated as "Principal Officer" as required under provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, from time to time, to ensure compliance with the obligations under the Act and Rules.

In case any further information/clarification is required in this regard, the 'Principal Officer' as designated may be contacted.

SAVE
Inclusion-Growth-Prosperity

Annexure

Annexure A - Officially Valid Documents

SMPL 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 or the equivalent e-documents thereof 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

- 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.
- 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 SMPL.

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).
