ujjivan SMALL FINANCE BANK
Build a Better Life

KYC Policy Extract

1. Introduction

In the current economic scenario, it is imperative that appropriate measures are taken to prevent intentional/unintentional usage of the banking channels by criminal elements for money laundering or terrorist financing activities. Ujjivan Small Finance Bank Limited (hereinafter referred to as "the Bank") has developed robust Know Your Customer (KYC) principles and Anti-Money Laundering (AML) standards to know/ understand its customers and their financial dealings and manage risks arising out of such financial dealings prudently. Reserve Bank of India (RBI) has advised banks to put in place a Board approved KYC AML policy framework, which shall document the underlying principles for customer acceptance, customer identification, transaction monitoring and risk management. This document seeks the approval of the Board to renew the existing policy, incorporating and enhancing with revised and additional guidelines that have been introduced by the RBI and other regulators since last approval.

2. Objectives of the Policy

The policy aims to develop a diligent and compliance sensitive culture in the Bank through a focused approach on customer acceptance and identification procedures. The key objectives of the policy are as under:

1. Prevent the Bank from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities, through various channels, products and services it offers
2. Define a mechanism for risk categorisation of customers at the time of account opening and transaction monitoring measures commensurate with the risk categorisation of the customers
3. Enable the Bank to know/ understand its customers and their financial dealings better and manage its risks in a prudent manner
4. Allocate responsibility for effective implementation of policy
5. Develop a comprehensive Anti-money laundering (AML) / Combating Financing of Terrorism (CFT) programme in line with the regulatory requirements covering systems and controls, training of staff and management oversight and ensure its effective implementation

3. Applicability of the Policy

This policy will be applicable to all the customers, including both depositors and borrowers, of the Bank who avail any of the products and services offered by the Bank and shall also include walk-in customers meaning thereby people who do not have an account based relationship with the Bank, but undertake transactions by availing of products and services that are offered by the Bank.

This policy will be applicable to all the branches, Regional Offices and Business Correspondents (BCs)/ sub-agents of the Bank and will be read in conjunction with operational guidelines issued from time to time through circulars and a master Standard Operating Procedure document. This policy shall be read in conjunction with the Compliance Policy and Annexures to the KYCAML Policy.

4. Key Elements of the Policy

In line with the RBI guidelines, the KYC policy comprises the following components:

A) Customer acceptance
B) Customer identification
C) Transaction monitoring
D) Risk management.

- **Customer Acceptance**

The Bank's Customer Acceptance Policy (CAP) lays down the criteria for acceptance of customers.
A customer is any person who enters into any financial dealing or activity with the Bank and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
The customers may approach the Bank to avail of the products and services offered through branches, BCs/ agents or through digital channels such as mobile application and internet banking. All these channels:

- Accept customers only after verifying /authenticating their identity;
- Ensure necessary checks before opening a new account so that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations or whose name appears in the sanctions lists circulated by Reserve Bank of India and the Banks own internal list of negative customers. In the case of loan accounts this check is done post the opening of the account;
- Classify customers into various risk categories and, based on risk perception, apply the acceptance criteria for each category of customers;
- Will not open an account or close an existing account (except as provided in this Policy), where identity of the account holder cannot be verified and/ or

documents/ information required could not be obtained/ confirmed, as per the risk categorization, due to non-cooperation of the customer or non-reliability of the data/ information furnished to the Bank.

- While opening the bank accounts for these customers, the Bank uses multiple sources such as e-KYC service of UIDAI, mobile banking and tab banking to capture the KYC details of the customer along with the required KYC documents;
- Not to allow existing customers to continue or accept new customers if they are on the United Nations Sanctions, Office of Foreign Assets Control (OFAC) list and any other lists prescribed by the relevant regulators;
- Open accounts for PEPs after clearance from Head Business and Chief Compliance Officer and monitor operations in such accounts on an on-going basis;
- All customer accounts deemed to be high risk to be opened with the specific approval of RBMs.
- Prohibit the opening of anonymous or fictitious/ benami accounts;
- Shall have in place suitable built-in safeguards to avoid harassment of the customer.
- The Implementation of CAP should not become restrictive so as to result in denial of banking services to general public, especially to those who are financially or socially disadvantaged. The Channels also ensure that:
    - No transaction or account- based relationship is undertaken without following the Customer Due Diligence (CDD) procedure. CDD procedure in account opened using OTP based E KYC in non-face to face mode should be completed within a year. If the CDD procedure is not completed within a year, accounts shall be closed immediately and in respect of the borrowal accounts, no further debit shall be allowed.
    - The mandatory information is sought for KYC purpose while opening an account and during the periodic updating, as specified
    - CDD Procedure is followed for all the joint account holders, while opening a joint account
    - Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out
    - Optional'/additional information is obtained with the explicit consent of the customer after the account is opened
    - CDD procedure at UCIC level. Thus if an existing KYC compliant desires to open another account or avail any other product or service with the Bank,there shall be no need for a fresh CDD Exercise, as far as identification of the customer is concerned, subject if there is no change in demographic details of the customer

- CIFs with no active relationship more than 2 years to be tagged as inactive. In case of any new account opening for such inactive customers, applicable documents to be collected again.
- Exceptions related to customer acceptance shall be reviewed on case to case basis and Chief Compliance Officer may approve the case and subsequently present those cases to Executive Committee (EC)/ Risk Management Committee (RMC) for ratification/approval.
- 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
- Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority
- Where an equivalent e-document is obtained from the customer, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
- Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing Authority.
- Where the Bank is suspicious of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR

- **Risk Category and Customer Profile**

The Bank prepares a profile for each new customer based on risk categorization as mentioned in this policy. Based on the risk profile, the customers are classified into Low risk, Medium risk and High-risk category of customers. Detailed criteria for risk categorization of customers are provided in the annexure 3 to this policy. Bank shall periodically review risk categorization of customers and the need for applying due diligence measures. Such reviews will be conducted at least once in 6 months. The customer data of June and December of every year shall be reviewed for periodic review of Risk categorization.

Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash,

cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in

The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer

Enhanced due diligence is required for the customers who are classified under High risk category based on the KYC risk rating. Below are the EDD measures applicable for all High risk customers.

1. Contact Point Verification by branch is mandatory for all High- risk accounts.
2. All customer accounts deemed to be high risk to be opened with the specific approval of Regional Business Managers.
3. Bank may seek an additional information about customer's identification, nature of business activity, risk profile, information about their source of funds etc.
4. In case of PEP, obtain the summary of PEP, family background, source of fund etc.
5. Accounts for PEPs will be opened only after obtaining approval from Head Business and Chief Compliance Officer of the Bank.
6. The first payment is to be effected through the customer's KYC-complied account with another bank, for enhanced due diligence for non-face to face customers(Other than Aadhaar OTP based on boarding)
7. As a risk-mitigating measure for such accounts, REs shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. REs shall have a board approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts, wherein the Policy refers to the adherence to the Operational procedure in changing the mobile number as specified in SOP titled " **Due Diligence Process for linking and updating Mobile Number**

- **Enhanced due diligence (non-face to face customer onboarding)**

1. Certain additional enhanced due diligence measures have been including - RE shall verify the current address through positive confirmation before allowing operations in the account, PAN shall be obtained from the customer and shall be verified, customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced

monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP, etc.

2. Customers on-boarded through V-CIP/Video KYC shall be treated on par with face-to-face CIP.
3. In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening.
4. First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
5. Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP
6. FCU verification should be done for the accounts which are tagged as 'High'
7. As a risk-mitigating measure for such accounts, REs shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. REs shall have a board approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts, wherein the Policy refers to the adherence to the Operational procedure in changing the mobile number as specified in SOP titled " **Due Diligence Process for linking and updating Mobile Number"**

- **Customer Identification Procedure**

Customer identification means undertaking client due diligence measures while commencing an account-based relationship including identifying and verifying the customer, authorised signatory, the beneficial owner and the Power of Attorney holders on the basis of Officially Valid Documents (OVDs) as defined by RBI which may be obtained physically or through e-KYC procedure of UIDAI. The Bank, through its Officials or BCs/ agents, obtains sufficient information to establish identity of each new customer, whether regular, occasional or walk-in satisfies itself about the intended nature of the banking relationship and to satisfy the regulatory authorities in the future that appropriate due diligence was observed. The Bank has adopted a risk based approach to facilitate a customer friendly regime for identification of customers and to reduce costs and avoid hardship to customers, in particular the low-risk customers.

This policy seeks to address the below aspects of customer identification:

1. Lay down detailed procedures for identification of the customers at various stages, which may include:
   a. While establishing banking relationship
   b. While carrying out a financial transaction
   c. When the Bank will have doubt on the authenticity and adequacy of customer data it has obtained
   d. When selling third party products as agents
   e. While selling Banks' own products, sale and reloading of prepaid (*currently the Bank does not have such a product) and any other product for more than Rs. 50,000/-.
   f. When carrying out transactions for a non-account- based customer, that is a walk-in customer, where the amount involved is less than equal to Rs 50000/- as a single transaction or exceeds Rs. 50,000/-, as series of transactions, that appear to be connected.
   g. When there is a reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000/-

2. All customers on-boarded shall undergo Restricted Entity Check (Customer Name Screening) a process of determining whether Bank's existing or potential customers are part of any blacklists or regulatory lists or internal negative lists. The detailed procedural aspects of screening systems/procedure, alert handling/closure, quality check are included in the KYC AML CFT procedure manual.
3. In the case of all High Risk customers and on a random sampling basis in the case of Medium and Low Risk customers, rely on additional customer due diligence done by a third party (the FCU process) subject to the following conditions:

   (a) Necessary information of such customers' due diligence carried out by the third party is immediately obtained by the Bank.
   (b) Adequate steps are taken by the Bank to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
   (c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
   (d) The third party shall not be based in a country or jurisdiction assessed as high risk.

(e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Bank.

However, decision-making functions of determining compliance with KYC norms shall not be outsourced.

4. After opening the account, seek additional information from the customer if the Bank is not satisfied with the genuineness of the customer and the perceived risk in opening the account is high.

5. Each Customer including walk-in customer has to be tagged under Unique Customer Identification Code (UCIC) in order to avoid multiple identities of the same customer, track the products offered, monitor transactions in a holistic manner.

6. KYC verification /CDD of the office bearers are required and CDD shall not be required for all the members of SHGs while opening Saving Accounts. However, customer due diligence (CDD) of all the members of SHG may be undertaken at the time of credit linking of SHGs.

7. Bank had adopted JLG (Joint Lending Group) model in the Micro Banking segment for granting of loans. However, under JLG model, the individual KYC of the customers is obtained as part of the Customer acceptance."

Ensure that transactions above INR 50,000/- are effected by debit to customer's account or against cheques and not cash payments.

8. **Period for presenting payment instruments**

Payment of cheques/drafts/pay orders/banker's cheques, if they are presented beyond the period of three months from the date of such instruments, shall not be made.

Procedural aspects for customer acceptance and identification are given in annexure 2 to this policy.

- **V- CIP (Video Based customer identification Process)**

Bank shall undertake Video Based customer identification process and due diligence(CDD) measures in case of new individual customers on boarding, proprietor in case of proprietorship firm, Authorised signatories and Beneficial Owners (BOs) in case of Legal entity customers.

- **Definition of V-CIP**

Video based Customer Identification Process (V-CIP) is an alternate method of customer identification with facial recognition and customer due diligence by an authorised official of the Bank by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face Customer Identification Process.

Bank may undertake V-CIP to carry out:

- CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers. Provided that in case of CDD of a proprietorship firm, Bank shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned Policy, apart from undertaking CDD of the proprietor.

- Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication.

- Updation/Periodic updation of KYC for eligible customers.

- **Transaction Monitoring**

Transaction monitoring is an essential and critical aspect of due diligence and is required in order to monitor and reduce potential money laundering, terrorist financing and fraud related exposure of the Bank. It involves identifying and reviewing unusual or unrelated or suspicious transactions on an ongoing basis based on risk categorization of customers. All the transactions are monitored closely by the AML cell of the Bank to ensure that they are consistent with customer’s profile and source of funds.

The Bank has the following methods of monitoring.

- Monitoring of in-built thresholds and limits. This is periodically reviewed and modifications are made by MLRO
- On-going Due Diligence" means regular monitoring of transactions in accounts to ensure that those are consistent with RE's knowledge about the customers, customers' business and risk profile, the source of funds / wealth
- Continuous risk categorization of customers with due diligence
- Monitoring of high risk categorized customers
- Maintaining all the records pertaining to wire transfers / suspicious transactions
- Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
- Transactions which exceed the thresholds prescribed for specific categories of accounts.
- High account turnover inconsistent with the size of the balance maintained
- Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts

The extent of monitoring is aligned to the risk category of the customer.

- **Risk Management**

Banks are required to 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 periodicity of the ML/TF risk assessment exercise may be determined by, either the 'Board or 'a Committee of the Board' to which the power is delegated.

Bank shall apply a Risk Based Approach (RBA) and implement a CDD programme, having regard to the ML/TF risks identified (by the RE itself or through the National Risk Assessment) and the size of business, for mitigation and management of the identified risk and should have Board approved policies, controls and procedures in this regard. Further, REs shall monitor the implementation of the controls and enhance them if necessary."

Bank has developed a Standard Operating Procedure as addendum to KYC & AML Procedure Manual covering the risk assessment framework and methodology.

- **Periodical Review of Customer Identification Data**

1. Periodic updating means steps taken to ensure that documents, data or information collected under the customer due diligence process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the RBI.

2. Bank shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high-risk."

3. The Bank conducts revalidation of KYC, which includes confirming identity and address of the customer, assessment of risk profile of the customer based on the last updated KYC and seeking additional data, if required, from the customer. Timeframe for such revalidation is as under and applies from the date of account opening/ last KYC updation.

Risk Categorization	Periodicity (At least)
High Risk Customers	Every two years
Medium Risk Customers	Every eight years
Low Risk Customers	Every ten years

a) Individual customers:

i. **No change in the KYC information**: In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through branch visit, Internet and Mobile Banking and other applicable channels in the Bank.

ii. **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 through branch visit, Internet and Mobile Banking and other applicable channels. The declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables.
Further, a copy of OVD or deemed OVD.

iii. **Accounts of customers, who were minor at the time of opening account, on their becoming major:** In case of customers for whom

account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the Bank. Wherever required, Banks may carry out fresh KYC of such customers i.e. customers for whom account was opened when they were minor, on their becoming a major.

b) **Customers other than Individuals:**

i. **No change in KYC information:** In case of no change in the KYC information of the Legal entity customer, a self-declaration in this regard shall be obtained from the Legal entity customer through its email id registered with the Bank, ATMs, digital channels (such as online banking / internet banking, mobile application of Bank), letter from an official authorized by the Legal entity in this regard, board resolution etc. Further, Bank shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.

ii. **Change in KYC information:** In case of change in KYC information, Bank shall undertake the KYC process equivalent to that applicable for on-boarding a new Legal entity customer.

Additional measures: In addition to the above, Bank shall ensure:

- The KYC documents of the customer as per the current CDD standards are available with the Bank. This is applicable even if there is no change in customer information but the documents available with the Banks are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the Bank has expired at the time of periodic updation of KYC, Bank shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.
- Customer's PAN details, if available with the Bank, is verified from the database of the issuing authority at the time of periodic updation of KYC.
- Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the Bank and an intimation, mentioning the date of updation of KYC details, is provided to the customer.
- Bank shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, which

otherwise are not mandated under the above instructions, adopted by the Bank such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the Bank where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc.

- Bank shall send 3 notices to customers intimating that their operative accounts maintained with the Bank shall be frozen for operations, on account of failure in completion of the periodic KYC /re-KYC exercise. These 3 notices shall be sent with 30 days gap between each notice i.e. notices shall be sent consecutively for 3 months to the customers. If customer(s) fail to complete periodic KYC/Re-KYC exercise, the operations in the accounts of such customers shall be frozen till customers adhere to the norms of periodic KYC / Re-KYC .

.

- **Obligation of Secrecy**

The Bank has an obligation to maintain secrecy of the details of the account-holder, not only when the account holder has a relationship with the Bank, but also after the account is closed. This right of the customer to expect secrecy is limited in the following situations:

- Under provisions of various acts (Income Tax / Companies Act / RBI Act / FEMA etc)
- Based on customer's express or implied consent Disclosure with Business Correspondent / Business Facilitator
- Disclosure in Bank's interest
- Where there is a duty to the public to disclose

8. Combating Financing of Terrorism

- The Bank shall ensure to update the consolidated list of individuals and entities approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) circulated by the Reserve Bank.

- The Bank shall further scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the two lists. Full details of accounts bearing resemblance with any of the individuals/

entities in the list shall immediately be intimated to the Reserve Bank, MHA and FIU-IND.

- The Bank has its own data base of Negative Customers. Accounts of such customers will not be opened by the Bank and this data base will be periodically checked against any official list or list of PEPs and updated as required.

- **Reporting Requirements**

All cash transactions of Rs10 lakhs and above, are reviewed by AML team and In respect of suspicious transactions, the branches apart from reporting to their controlling office, will also report to the AML/Compliance officer at Head Office. The designated officer at the Head – Office shall report to the law enforcement authorities.

Reporting to Financial Intelligence Unit-India (FIU-IND)

Bank shall be in adherence to all the Regulatory and Statutory Reporting as mandated by FIU India.

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

Bank shall be in adherence to all applicable guidelines of CERSAI under CKYC Registry updation and sharing of the KYC information with CKYC Registry.

Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards

Bank shall be in adherence to all applicable provisions FATCA and Common Reporting Standards.

Training and awareness

Bank shall adopt training to its staff for creating awareness and also inform customers on the KYC requirements including that of periodic KYC requirement and also create awareness on the matters of customer transactional safety.

Monitoring of Transaction Monitoring & Reporting

Bank shall adopt and ensure all the extant Regulatory (RBI and Quazi Regulators) and Statutory guidelines like Prevention of Money Laundering Act (PMLA) 2002 FIU India etc (amended from time to time).