‘Know Your Customer’ (KYC) Standards and ‘Anti Money Laundering’ (AML) / Combating the Financing of Terrorism (CFT) Policy

History of Revisions

Version	Summary of Revisions	Date of Approval
1.7	Regulatory Changes	28-01-22
1.6	Regulatory Changes	17-Jun-21
1.5	Regulatory Changes	17-Sep-20
1.4	Regulatory Changes	07-Nov-19
1.3	Annual Review	31-Jan-19
1.2	Annual Review	12-Mar-18
1.1	Policy Formulation	04-Sep-16

Table of Contents

1. Preamble

1.1 Objective of the Policy

The objective of this Policy is to provide a comprehensive KYC/AML framework, which will enable the Bank to implement a robust procedures and controls in line with the applicable laws in India with reference to Money Laundering / CFT and adhere to standards accepted internationally by the financial sector on the subject.

1.2 Scope of the Policy

This policy is applicable to all related activities of all branches/offices of the Equitas Small Finance Bank, hereinafter referred to as 'Bank' and is to be read in conjunction with detailed related operational guidelines / annexures and instructions issued by RBI / Government of India from time to time.

2. Regulatory Framework Applicable Regulations

2.1 Master Direction - Know Your Customer (KYC) Direction, 2016 (Updated as on May 10, 2021)

2.1.1 KYC Policy

Bank should frame their KYC policies incorporating the following four key elements:

a. Customer Acceptance Policy (CAP);
b. Customer Identification Procedures (CIP);
c. Monitoring of Transactions; and
d. Risk Management.(Clause 3 of the Circular)

2.1.2 Money Laundering and Terrorist Financing Risk Assessment.

Banks shall 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 risk assessment exercise shall be determined by the Board of the Bank, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

The Bank shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and shall have Board approved policies, controls and procedures in this regard. Further, the Bank shall monitor the implementation of the controls and enhance them if necessary (Clause 5A).

2.1.2.1 Reporting Requirements

Reports to be furnished to FIU-IND by the Bank

a. Cash Transaction Report (CTR)
b. Suspicious Transaction Reports (STR)
c. Non-Profit Organisation Transactions

d. Cross-border Wire Transfer .(Chapter 8 of the circular)

2.1.3 General Guidelines

Bank to ensure the following subjects as per extant guidelines

a. Confidentiality of customer information
b. Avoiding hardship to customers
c. Sensitising customers
d. Hiring of Employees
e. Employee training
f. Provisions of FCRA
g. Applicability to overseas branches/subsidiaries
h. Technology requirements
i. Designated Director
j. Principal Officer (Clause 9 of the circular)

2.2 Master Directions on Prepaid Payment Instruments (PPIs) dated August 27, 2021

2.2.1 Full-KYC PPIs

The Video-based Customer Identification Process (V-CIP), as detailed in Department of Regulation's Master Direction on KYC dated February 25, 2016 (as amended from time to time), can be used to open full-KYC PPIs as well as to convert Small PPIs **(or Minimum-detail PPIs)** into full-KYC PPIs (Clause 9.2)

3 ESFB Policy framework

3.1 Introduction

a. In terms of the Guidelines issued by the Reserve Bank of India (RBI) on Know Your Customer (KYC) norms, and Anti Money Laundering (AML) measures and combating of financing of Terrorism (CFT) obligations from time to time; Banks are required to put in place a comprehensive policy framework covering KYC norms, AML Measures and combating of financing of Terrorism (CFT) obligations.

b. The Know your customer guidelines issued by the RBI take into account the recommendations made by the Financial Action Task Force (FATF) on AML Standards and on combating financing of terrorism.

c. The guidelines also incorporate Financial Action Task Force (FATF) recommendations on AML/ CFT, and Basel Committee on Banking Supervision (BCBS) guidelines require Banks to adopt 'Know Your Customer' and 'Customer Due Diligence' processes for the customers who avail their products/ services.

d. This policy document is prepared in line with the RBI guidelines and incorporates the Bank's approach to customer identification procedures, customer profiling based on the risk perception and monitoring of transactions on an ongoing basis.

3.2 Purpose

a. Enable the Bank to conduct clean, commercial business conforming to standards set by the Banking Industry; within the framework of the relevant regulations and laws.

b. To prevent the Bank's business channels/products/services from being used as a channel for money laundering.

c. To establish a framework for adopting appropriate AML procedures and controls in the operations / business processes of the Bank.

d. To report and take suitable action, upon detecting the suspicious activity involving shades of money laundering as directed by regulators and Head office from time to time.

e. To comply with applicable laws in India with reference to money laundering/CFT and adhere to standards accepted internationally by the financial sector on the subject.

3.3 Money Laundering – Risk Perception

Money laundering exposes the Bank to various risks such as:

a. Reputation Risk: Risk of loss due to severe impact on Bank's reputation. This can be of particular concern given the nature of the bank's business, which requires the confidence of depositors, creditors and the general market place.
b. Compliance Risk: Risk of loss due to failure of compliance with key regulations governing the bank's Operations.
c. Operational Risk: Risk of loss resulting from inadequate or failed internal processes, people and Systems or from external events.
d. Legal Risk: Risk of loss due to any legal action, the bank or its staff can face due to failure to comply with the law.

3.4 Key Elements of the Policy

The KYC / AML / CFT policy includes following four key elements:

3.4.1 Customer Acceptance Policy (CAP)

3.4.2 Customer Identification Procedures (CIP)

3.4.3 Customer Due Diligence (CDD) Procedure

3.4.4 Monitoring of Transactions

3.4.5 Risk Management

3.4.1 Customer Acceptance Policy (CAP)

3.4.1.1 In line with the Bank's policy to conduct clean, commercial business conforming to extant guidelines of statutory bodies and regulators and to prevent the Bank's business channels/products/services from being used as a channel for money laundering/ terrorist financing, the Bank will exercise due care and caution in establishing customer relationships and in conducting transactions for random walk-in customers. The main elements of the Bank's Customer Acceptance Policy are enunciated below.

3.4.1.2 As part of the Customer Acceptance Policy, the Bank will verify the identity as laid down in Customer Identification Procedures and ensure that:

i. No account is opened in anonymous or fictitious / Anonymous / benami name.
ii. No account on behalf of other persons whose identity has not been disclosed or cannot be verified is opened.
iii. No accounts are opened of known criminals or banned entities.
iv. No accounts are solicited of Shell Banks / Companies.
v. No account is opened where the Bank 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.
vi. No transaction or account-based relationship is undertaken without following the CDD procedure.
vii. The mandatory information sought for KYC purpose while opening an account and during the periodic updation, is specified.
viii. 'Optional' / additional information is obtained with the explicit consent of the customer after the account is opened.
ix. CDD Procedure is followed for all the joint account holders, while opening a joint account.
x. Circumstances in which, a customer is permitted to act on behalf of another person / entity, are clearly spelt out.
xi. No account is opened where identity of the customer matches with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
xii. The PAN details will be verified from the database of the issuing authority.
xiii. Parameters of risk perception are clearly defined in terms of the nature of business activity, location of the customer and his clients, mode of payments, volume of turnover, social and financial status, etc. so as to enable the Banking categorizing the customers into high, medium and low risk.
xiv. CDD procedure will be carried out at the UCIC level. Thus, if an existing KYC compliant customer of the Bank desires to open another account with the Bank, there will be no need for a fresh CDD exercise.

3.4.1.3 Apart from adhering to the above for opening of accounts, the Bank will ensure these prohibitions are observed while carrying out any type of transaction including cross-border transactions like remittances under various schemes, trade related transactions, money changing activities, etc. for persons not having an account with the Bank. Similarly, these guidelines will also apply in respect of Demat accounts opened by the Bank as Depository Participant, and the transactions carried out as Merchant Banker, and Banker to Issue.

3.4.1.4 The Bank will have suitable systems in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the United Nations Security Council (UNSC) – "ISIL (Da'esh) &Al-Qaida Sanctions List", The "1988 Sanctions List" and other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time

3.4.1.5 The Bank will ensure that the adoption of customer acceptance policy and its implementation is not too restrictive which can result in denial of banking facility to the members of the general public, especially to those, who are financially or socially disadvantaged.

3.4.1.6 Risk Perception in respect of Customer:

"Customer risk" in the present context refers to the money laundering and terrorist funding risk associated with a particular customer from a Bank's perspective. This risk is based on risk perceptions associated with customer profile and level of risk associated with the product and channels used by the customer.

3.4.1.7 For categorizing a customer as high risk, medium risk and low risk, the Bank will consider the following parameters:

a. Customer Constitution: Individual, Proprietorship, Partnership, Private Ltd. etc.
b. Business Segment: Retail, Corporate etc.
c. Country of residence/Nationality: Whether India or any overseas location/Indian or foreign national.
d. Product Subscription: Salary account, NRI products etc.
e. Economic Profile: HNI, Public Ltd. Company etc.
f. Account Vintage: Less than six months old etc.
g. Presence in regulatory negative/PEP/Defaulters/Fraudster lists.
h. Suspicious Transaction Report (STR) filed for the customer.
i. AML alerts.

3.4.1.8 Other parameters like source of funds, occupation, purpose of account opening, nature of business, mode of operation etc. can also be used in addition to the above parameters. Bank will adopt all or majority of these parameters on a need basis.

3.4.1.9 All customer profiles/accounts of HNIs, PEPs, NGOs, Trusts, Co-operative Societies, HUF, Exporters, Importers and Accounts having Beneficial Owners will be invariably categorized as High Risk, irrespective of the lower risk category (low/medium) allotted under other parameters in the Matrix like customer profession, type of business, product code, account status, account vintage and balance in the account.

3.4.1.10 Customers who are named in complaints (from legal enforcement authorities)/frauds will be categorized as high risk.

3.4.1.11 Blocked Accounts and unclaimed deposits will be categorized as high risk.

3.4.1.12 Accounts of dealers in Jewellery, gold/silver/bullions, diamonds and other precious metals/stones will be categorized under high risk.

3.4.1.13 Under the parameter of customer vintage on system, newly opened CASA accounts which have not completed 6 months will be categorized as high risk, except accounts pertaining to staff, ex-staff, pensioners, Small Accounts, Financial Inclusion and Basic Savings Bank Accounts.

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

3.4.1.15 Below is an indicative guideline of customers who can be classified as high, medium and low risk based on the Customer Risk Categorization (CRC) guidelines issued by IBA:

a. High Risk Customers:

For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his client profile, etc. besides proper identification. Bank will subject such accounts to enhanced monitoring on an ongoing basis.

The following are classified as high-risk customers:

i. Trusts, charities, NGOs and organizations receiving donations.
ii. Companies having close family shareholding or beneficial ownership
iii. Firms with 'sleeping partners'.
iv. Accounts under Foreign Contribution Regulation Act.
v. Politically Exposed Persons (PEPs).

vi. Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner.
vii. Those with dubious reputation as per public information available.
viii. Accounts of non-face-to-face customers, etc.
ix. High Net worth Individuals
x. Accounts of Cash intensive businesses such as accounts of bullion dealers (including sub-dealers) and jewelers.
xi. NRI's residing in FATF non-compliant countries.

b. Medium Risk Customers:

Customers who are likely to pose a higher than average risk to the bank will be categorized as medium or high risk. For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his/her client profile, etc. besides proper identification.

The following are classified as medium risk customers:

i. Gas Dealers
ii. Car/boat/plane dealers
iii. Electronics (wholesale)
iv. Travel agency
v. Telemarketers
vi. Telecommunication service providers
vii. Pawnshops
viii. Auctioneers
ix. Restaurants, Retail shops, Movie theatres, etc.
x. Sole practitioners
xi. Notaries
xii. Accountants
xiii. Blind
xiv. Purdanashin
xv. NRI's residing in FATF compliant countries.

c. Low Risk Customers:

Individuals and entities whose identities and sources of income can be easily identified and transactions in whose accounts mostly conform to the known profile can be categorized as low risk, such as:

i. Salaried employees
ii. People belonging to lower economic strata of the society
iii. Government Departments
iv. Government owned companies
v. Regulatory and Statutory bodies

For the above category, the KYC requirements of proper identification and verification of proof of address will suffice.

3.4.1.16 The above categorization of customers under risk perception is only illustrative and not exhaustive. The Bank can categorize the customers according to the risk perceived by them while taking into account the above aspects.

3.4.1.17 The Bank will be guided by the indicative list provided by IBA of High/Medium risk Products, Services, Geographies, locations, etc., for Risk Based Transaction Monitoring by Banks (detailed in Annexure II).

3.4.2 Customer Identification Procedure (CIP)

3.4.2.1 Financial Action Task Force (FATF) recommendations on AML/ CFT, and Basel Committee on Banking Supervision (BCBS) guidelines require banks to adopt 'Know Your Customer' and 'Customer Due Diligence' processes for the customers who avail their products/ services.

Customer identification means undertaking client due diligence measures while commencing an account-based relationship including identifying and verifying the customer and the beneficial owner based on one of the Officially Valid Documents (OVDs). "Officially Valid Document" means documents as defined in the Master Direction.

The Bank will obtain sufficient information to establish, to its satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of the Banking relationship. In respect of customers where the level of risk is perceived to be relatively higher, additional information will be obtained. Customer Identity will also be verified in respect of such customers who only avail Third Party Products sold by the Bank as agent/ distributor.

3.4.2.2. By undertaking adequate client due diligence measures the Bank will be able to satisfy the competent authorities that due diligence was carried out based on the risk profile of the customer in Compliance with the extant guidelines in place

3.4.2.3 The Bank will carry out Customer Identification/ Customer Due Diligence procedures at various stages as indicated below.

i. Commencement of an account-based relationship with the customer.
ii. When the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.
iii. Selling third party products as agent, selling its own products, / sale and reloading of prepaid cards and any other product for more than rupees fifty thousand.
iv. Carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
v. When Bank has 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 rupees fifty thousand.
vi. While doing KYC updation, the Bank will apply customer due diligence measures to existing clients at an interval of two /eight / ten years in respect of high/medium/ low risk clients respectively.
vii. Other 'optional' customer details/additional information, if required can be obtained separately after the account is opened only with the explicit consent of the customer.

3.4.2.4 The Bank will collect the PAN / form 60 or equivalent e-document at the time of on-boarding as per the RBI Directions. In case existing customer on account of any injury, illness or infirmity on account of old age or otherwise, and such like causes where the customer is unable to provide the PAN / form 60, the Bank can allow continued operations of the account on a case to case basis. However, such accounts shall be subjected to enhanced monitoring.

3.4.2.5 If the Bank at any point in time relies on a third party for verifying the identity of customers during commencement of a relationship, it will ensure that:

i. Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
ii. Adequate steps are taken by the Bank to satisfy that the copies of the identity proofs and data collected is made available to the Bank immediately upon request.
iii. The Bank has adequate procedures and policy in place to monitor, supervise to regulate the third party in line with due diligence requirements and preservation of records.
iv. The third party is not based out of a jurisdiction or country which is high risk.
v. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures is with the Bank.
vi. Bank will not engage third party for verifying of Accounts of Politically Exposed Persons (PEPs).

3.4.2.6 Video based Customer Identification Process (V-CIP)": is an alternate method of customer identification with facial recognition and customer due diligence by an 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. The V-CIP will be treated as face-to-face process as per the Master Direction.

The Bank shall undertake V-CIP to carry out:

i) 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. In case of CDD of a proprietorship firm, the Bank shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as per the existing guidelines, apart from undertaking CDD of the proprietor.

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

iii) Updation/Periodic updation of KYC for eligible customers.

iv) To open full-KYC Prepaid Payment Instruments (PPIs).

v) Conversion of Small PPIs of into full-KYC PPIs.

The Bank while opting to undertake V-CIP, shall adhere to the following minimum standards:

(a) V-CIP Infrastructure

(i) The Bank shall comply with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure should be housed in the Bank's own premises and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process shall be compliant with relevant RBI guidelines.

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

(iii) The V-CIP infrastructure / application shall be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

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

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

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

(vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

(viii) The V-CIP application software and relevant APIs / webservices shall also undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

(b) V-CIP Procedure

(i) The Bank shall formulate a clear work flow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process shall be operated only by officials of the Bank specially trained for this purpose. The official should be capable to carry out liveliness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it.

(ii) If there is a disruption in the V-CIP procedure, the same shall be aborted and a fresh session initiated.

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

(iv) Any prompting, observed at end of customer shall lead to rejection of the account opening process.

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

(vi) The authorised official of the Bank performing the V-CIP shall record audio-video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

a) OTP based Aadhaar e-KYC authentication

b) Offline Verification of Aadhaar for identification

c) KYC records downloaded from CKYCR, in accordance with the RBI Direction, using the ifier provided by the customer.

d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through DigiLocker RE shall ensure to redact or blackout the Aadhaar number in terms of the extant guidelines.

In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.

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

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

(viii) The Bank shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through DigiLocker.

(ix) Use of printed copy of equivalent e-document including e-PAN is not valid for the V-CIP.

(x) The authorised official of the Bank shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e-PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.

(xi) Assisted V-CIP is permissible with the help of Banking Correspondents (BCs) facilitating the process only at the customer end. The Bank shall maintain the details of the BC assisting the customer, where services of BCs are utilized. However, the ultimate responsibility for customer due diligence will be with the bank.

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

(xiii) All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by the Bank.

(c) V-CIP Records and Data Management

(i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. The Bank shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in the Master Direction, shall also be applicable for V-CIP.

(ii) The activity log along with the credentials of the official performing the V-CIP shall be preserved.

3.4.3 Customer Due Diligence (CDD) Procedure

'Due Diligence' goes beyond merely establishing identity of the customer. It includes ascertaining certain information about the customer as considered appropriate and necessary for the nature of banking relationship with the customer. The extent of 'due diligence' carried out will depend on the risk perception of the customer.

a. Accounts of individuals:

   i. For opening accounts of individuals, Branches will obtain one certified copy of an "Officially Valid Document", containing details of identity and address, one recent photograph and such other documents pertaining to the nature of business and financial status of the customer.

   ii. If Aadhaar is taken as an OVD, the Bank will ensure that customer redacts or blackout the first 8 digits of his Aadhaar number.. E-KYC authentication will be carried out on voluntary basis at the time of on-boarding and with customer consent. Bank will obtain the Customer's Aadhaar for Aadhaar seeding.

b. Introduction of Accounts:

Since introduction from an existing customer is not necessary for opening accounts under PML Act and Rules or the RBI's extant instructions, the Bank will not insist on introduction for opening of bank accounts.

c. Basic Savings Bank Deposit Accounts:

The Bank will have appropriate procedures to provide "Basic Savings Bank Deposit Account" to all the customers. The Basic Savings Bank Deposit Account will be considered a normal banking service available to all. This account will not have the requirement of any minimum balance. The services available in the account will include deposit and withdrawal of cash at bank branch as well as ATMs; receipt/credit of money through electronic payment channels or by means of deposit/ collection of cheques drawn by Central/ State Government agencies and departments.

While there will be no limit on the number of deposits that can be made in a month, account holders will be allowed a minimum of four withdrawals in a month, including ATM withdrawals; and facility of ATM card or ATM-cum-Debit Card.

The above facilities will be provided without any charges. Further, no charge will be levied for non-operation/ activation of inoperative Basic Savings Bank Deposit Account. Additional value added services beyond the stipulated basic minimum services are chargeable.

The Basic Savings Bank deposit Account will be subject to RBI instructions on Know Your Customer (KYC)/ Anti-Money laundering (AML) for opening of bank accounts issued from time to time.

Holders of Basic Savings Bank Deposit Account will not be eligible for opening any other savings bank deposit account in the Bank. If a customer has any other existing savings bank deposit account in the Bank, he/she will be required to close it within 30 days from the date of opening the account.

d. Small Accounts:

An individual who desires to open a small account in the Bank can be allowed to open such an account on production of a self-attested photograph and affixation of signature or thumb print, as the case can be, on the Account Opening Form in which:

i. the aggregate of all credits in a financial year does not exceed rupees one lakh;
ii. the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and
iii. the balance at any point of time does not exceed rupees fifty thousand.

Provided that this limit on balance will not be considered while making deposits through Government grants, welfare benefits and payment against procurements.

Further, small accounts are subject to the following conditions:

1. The bank will obtain a self-attested photograph from the customer
2. The Officer / Manager / Sr. Manager of a branch of the Bank [authorized as "Designated Officer" for the purpose of opening of small account], while opening the small account will certify under his signature that the person opening the account has affixed his signature or thumb impression, as the case can be, in his presence. Provided that where the individual is a prisoner in a jail, the signature or thumb print will be affixed in presence of the officer in-charge of the jail and the said officer will certify the same under his signature and the account will remain operational on annual submission of certificate of proof of address issued by the officer in-charge of the jail.
3. Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to such account and that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place.
4. The small accounts remains operational initially for a period of twelve months which can be extended for a further period of twelve months, provided the account holder applies and furnishes evidence of having applied for any of the OVDs during the first twelve months of the opening of the said account.
5. The entire relaxation provisions will be reviewed after twenty four months.

The small account will be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of client will be established through the production of officially valid documents. For small accounts, the identity of the customer will be validated with production of an OVD. Foreign remittance will not be allowed to be credited into the small account unless the identity of the customer is established through the production of OVD including PAN number / Form 60.

6. Customer due diligence will be carried out by the Bank's official. Only biometric e-KYC is permitted to be carried out by Business correspondent / facilitator.

e. Accounts of non-face-to-face customers:

In the case of non-face-to-face customers (i.e., customers who open accounts without visiting the branch/offices of the Bank or meeting the officials of the Bank), apart from applying the usual customer identification procedures, there will be specific and adequate procedures to mitigate the higher risk involved, as per the extant guidelines.

Certification / self-certification (list of circumstances for acceptance of self-certification for non-face to face accounts will be defined in the process note) of all the documents presented will be insisted upon and, if necessary, additional documents can be called for. In such cases, Bank can also require the first payment to be effected through the customer's account with another bank, which, in turn, follows KYC standards. In the case of cross border customers (NRIs / PIOs), there is the additional difficulty of matching the customer with the documentation and the Bank can have to rely on third party certification. In such cases, it will be ensured that the third party is any one of the following:

i. authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
ii. branches of overseas banks with whom Indian banks have relationships,
iii. Notary Public abroad,
iv. Court Magistrate,
v. Judge,
vi. Indian Embassy/Consulate General in the country where the non-resident customer resides.

f. Accounts of Foreign students studying in India:

The following procedure will be followed for opening accounts of foreign students who are not able to provide an immediate address proof while approaching the Bank for opening bank account:-

i. The Bank will open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with visa and immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.
ii. The Bank will obtain a declaration about the local address within a period of 30 days of opening the account and verify the said local address.
iii. During the 30 days period, the account will be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of monthly withdrawal to Rs.50,000/-, pending verification of address.
iv. The account will be treated as a normal NRO account, and will be operated in terms of instructions contained in the Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of Schedule 3 of FEMA Notification 5/2000 RB dated Can 3, 2000 and Circulars issued from time to time.
v. Students with Pakistani nationality will need prior approval of the Reserve Bank for opening the account.

g. Accounts of Politically Exposed Persons (PEPs)

Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/ Governments, senior politicians, senior

government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

For the purpose of this document, following are the broad classifications of a PEP:

i. All senior political and government leaders and functionaries including:
ii. Heads of State ranging from Royals to Presidents and Prime Ministers, Government Ministers and Deputy Ministers, as well as Political Party Leadership and all Members of Parliament, Local Legislatures
iii. City Mayors and governors
iv. Key Senior Government Functionaries of the Judiciary and Legislature
v. Senior Military Officers
vi. Ambassadors
vii. Key leaders of state-owned enterprises
viii. Heads of government agencies
ix. Heads of supranational bodies, e.g. UN, IMF, WB
x. Private companies, trusts or foundations owned or co-owned by PEPs, whether directly or indirectly.
xi. A current or former senior official in the executive, legislative, administrative, military, or judicial branch of a foreign government (elected or not);
xii. A senior official of a major foreign political party;
xiii. A senior executive of a foreign government owned commercial enterprise, being a corporation, business or other entity formed by or for the benefit of any such individual;
xiv. An immediate family member of such individual; meaning spouse, parents, siblings, children, and spouse's parents or siblings;
xv. Any individual publicly known (or actually known by the relevant financial institution) to be a close associate / personal or professional associate (in particular persons acting in a financial fiduciary capacity)

Risk & Mitigation

Relationships with PEPs can represent increased risks due to the possibility that individuals holding such positions can misuse their power and influence for personal gain or advantage, or for the personal gain or advantage of close family members and close associates. Such individuals can also use their families or close associates to conceal funds or assets that have been misappropriated as a result of abuse of their official position or resulting from bribery and corruption. In addition, they can also seek to use their power and influence to gain representation and/or access to, or control of, legal entities for similar purposes. PEPs are one of the high-risk categories of customers, particularly with regard to Money Laundering (ML).

Bank will procure information on each Politically Exposed Person that wishes to do business with the bank. The best time for the bank to obtain information on a Politically Exposed Person is when that person is attempting to open an account with the bank.

The Bank will gather sufficient information on any person / customer of this category intending to establish a relationship and check all the information available on such person in public domain.

The decision to open an account for a PEP will be taken at a senior level and such accounts will be opened with the approval of the Zonal Head or an official designated by the Head – Branch Banking / Inclusive Banking / Corporate Banking / MSME

In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, branch will obtain senior management's approval (Zonal Head or an official designated by the Head

– Branch Banking / Inclusive Banking / Corporate Banking / MSME) to continue the business relationship and subject the account to the CDD measures as applicable to PEPs including enhanced monitoring on an ongoing basis. These instructions are also applicable to accounts where a PEP is the ultimate beneficial owner.

Bank will also subject such accounts to enhanced monitoring on an on-going basis. To mitigate the risk of PEPs, the bank will gather more information about these persons and their family members and apply enhanced due diligence to include the following:

i. Identify the customer and the beneficial owner.
ii. Know the customer's country of residence.
iii. Review resources (such as available lists of names) to determine whether the customer is a PEP.
iv. Obtain information directly from the customer concerning the possibility of him becoming a PEP.
v. Know the objective of opening the account and the volume and nature of the activity expected for the account.
vi. Obtain information on the occupation and the other income sources.
vii. Know the source of wealth and funds.
viii. Obtain information about the direct family members or associates who have the power to conduct transactions on the account.
ix. Obtain senior management approval prior to on-boarding such customers
x. Have screening tools in place to identify PEPs as part of the existing base of customers.
xi. Identification of a PEP or their "Close Family Member or Close Associates

All such accounts opened, will be flagged as 'high' risk on system for periodic enhanced due diligence. Any declassification of a PEP will be subject to appropriate level of review and approval from business and compliance.

h. Other Guidelines

i. A customer is required to submit only one Officially Valid Document (OVD) for both proof of identity and for proof of address as part of KYC procedure. In case of officially valid document furnished by the client does not contain updated address, the customer can submit any of the following documents for the limited purpose of proof of address:

1. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
2. property or Municipal tax receipt;
3. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
4. 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 will need to submit an OVD with current address within three months of submitting the above documents. In all such cases, the bank will collect a declaration from the customer at the time of on boarding for adherence to this requirement.

5. Where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India will be accepted as proof of address.

Explanation: For the purpose of this clause, a document will 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.

ii. Obtaining fresh documents of customers when customers approaches for transferring their account from one branch of the Bank to another branch will not be required. KYC once done by one branch of the Bank will be valid for transfer of the account within the Bank if full KYC verification has been done for the concerned account and is not due for periodic updation. The customer will be allowed to transfer his account from one branch to another branch without restrictions.

iii. Transfer of existing accounts will be permissible without insisting on fresh proof of address and on the basis of a self-declaration from the account holder about his/her current address.

i. Accounts of persons other than individuals:

i. Accounts of Companies:
Where the customer is a company, one certified copy each of the documents mentioned under Annexure I are to be obtained for customer identification. The Bank will be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. The Bank will examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements can be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

ii. Accounts of Partnership firms:
Where the customer is a partnership firm, one certified copy each of the documents mentioned under Annexure I are to be obtained for customer identification.

iii. Accounts of Trusts:
Where the customer is a Trust, one certified copy each of the documents mentioned under Annexure I are to be obtained for customer identification.

iv. Accounts of Unincorporated association or a body of individuals:
Where the customer is an unincorporated association or body of individuals one certified copy each of the documents mentioned under Annexure I are to be obtained for customer identification.

v. Accounts of Proprietary Concerns:

1. For proprietary concerns, in addition to the OVD applicable to the individual (proprietor), any two of the documents in the name of the proprietary concern are required as mentioned under Annexure I.

2. Though the default rule is that any two documents, mentioned above, will be provided as activity proof by a proprietary concern, in cases where the Bank is satisfied that it is not possible to furnish two such documents, Branch Manager will have the discretion to accept only one of those documents as activity proof. In such cases, the Bank, however, will undertake contact point verification, collect such information as will be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern.

vi. For opening accounts of Government or its Departments, Societies, Universities and Local Bodies like Village Panchayats:
A certified copy of the following documents will be obtained:

1. Document showing name of the person authorized to act on behalf of the entity;
2. Officially Valid Documents for proof of identity and address in respect of the person holding a power of attorney to transact on its behalf and
3. Such documents as can be required by the Bank to establish the legal existence of such an entity/ juridical person.

vii. Customer accounts opened by professional intermediaries:

When the Bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client will be identified. Bank can hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Branches will not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Bank. Where funds held by the intermediaries are not co-mingled at the Bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners will be identified. Where such funds are co-mingled at the Bank, the Bank will still look into the beneficial owners. Where the Bank rely on the 'customer due diligence' (CDD) done by an intermediary, Bank will satisfy itself that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers. The ultimate responsibility for knowing the customer lies with the Bank.

viii. Beneficial Ownership:

1. Rule 9(3) of the Prevention of Money Laundering Rules, 2005 requires that every banking company, and financial institution, as the case can be, will identify the beneficial owner and take all reasonable steps to verify his identity. The term "Beneficial Owner" has been defined as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person.

2. A juridical person has been defined as an Entity(as a firm), that is not a single natural person(as a human being), authorized by law with duties and rights, recognized as a legal authority having a distinct identity, a legal personality (Also known as artificial person, juridical entity, juristic person, or legal person).

3. The procedure for determination of Beneficial Ownership as per RBI/Government guidelines is as under:

   i. Where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercises control through other means.
   Explanation. - For the purpose of this sub-clause-

   1."Controlling ownership interest," means ownership of or entitlement to more than twenty-five percent of shares or capital or profits of the company;

2. "Control" will include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

ii. Where the client is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of/entitlement to more than fifteen percent of capital or profits of the partnership;

iii. Where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;

iv. Where no natural person is identified under (i) or (ii) or (iii) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

v. Where the client is a trust, the identification of beneficial owner(s) will include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

vi. Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

vii. Where the client is a proprietorship firm, there is no separation between a proprietor and a proprietorship firm. CDD process of proprietor will suffice and no separate BO identification is required.

4. There exists the possibility that trust / nominee or fiduciary accounts can be used to circumvent the customer identification procedures. In such cases, Bank will determine whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary. If so, Bank will insist on satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. The different categories of beneficiaries will be identified as defined above. In the case of a 'foundation', steps will be taken to verify the founder managers / directors and the beneficiaries, if defined.

5. Accounts operated by Power of Attorney Holders/Letter of Authority Holders:
   i. In case of accounts operated by Power of Attorney (POA) Holders / Letter of Authority (LOA) Holders, KYC documents will be obtained from such POA holders/ LOA holders and records will be maintained/ updated in the system.

ix) Accounts of Non Profit Organizations:

A Non-Profit Organization (NPO) means any entity or organization that is registered as a Trust or a Society under the Societies Registration Act, 1860 or any similar State Legislation or a company registered under Section 8 of the Companies Act 2013.
All transactions involving receipts by these NPOs of value more than Rs.10 lac or its equivalent in foreign currency is to be reported to FIU-IND centrally from Head Office. However, if the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.10 lacs, the Bank will consider filing a Suspicious Transaction Report (STR) to FIU-IND.

x) Introduction of New Technologies - Credit cards / debit cards / smart cards / gift cards/Mobile Wallet/ Net Banking/ Mobile Banking/RTGS/ NEFT/ECS/IMPS etc.:

Bank will pay special attention to any money laundering threats that can arise from new or developing technologies including internet banking that might favor anonymity, and take measures, if needed, to prevent the same being used for money laundering purposes. The electronic cards (debit card, credit card, etc.) issued by the Bank to the customers can be used by them for buying goods and services, drawing cash from ATMs and electronic transfer of funds. Bank will ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. Bank will ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Further, where marketing of these cards is done through the services of agent, the agents will also to be subjected to due diligence KYC measures.

xi) Other Guidelines: For non-individuals, in case of transfer of account from one branch to another, the Bank would perform contact point verification and visit the premises and there is no requirement to collect documents in case accounts are KYC compliant.

j. Periodic updation of KYC:

i. CDD requirements for periodic updation:

The Bank will have a system of periodical updation of customer identification data (including photograph/s) as under:

Bank shall adopt a risk-based approach for periodic updation of KYC. However, periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC updation.

1. Individual Customers:

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

b) 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 Bank, customer's mobile number registered with the Bank, ATMs, digital channels (such as online banking / internet banking, mobile application of Bank), 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 Bank, 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.

c) 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, Bank 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

2. Customers other than individuals:
a) No change in KYC information: In case of no change in the KYC information of the customer, a self-declaration in this regard shall be obtained from the customer through its email id registered with the RE, ATMs, digital channels (such as online banking / internet banking, mobile application of RE), letter from an official authorized by the customer 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.

b) 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 customer.

3. Additional measures: In addition to the above, Bank shall ensure that –

a) 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 Bank 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.

b) 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.

c) An 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.

d) In order to ensure customer convenience, Bank may consider making available the facility of periodic updation of KYC at any branch.

e) The processes on updation / periodic updation of KYC shall be transparent and adverse actions against the customers shall be avoided, unless warranted by specific regulatory requirements.

3.4.4 Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC/AML procedures. The Bank will exercise ongoing due diligence with respect to every customer and closely examine the transactions to ensure that they are consistent with the customer's profile and source of funds as per extant instructions. The ongoing due diligence will be based on the following principles:

a. The extent of monitoring will depend on the risk category of the account. High risk accounts have to be subjected to more intensified monitoring.
b. The Bank will pay particular attention to the following types of transactions:

    i. large and complex transactions, and those with unusual patterns, which have no apparent economic rationale or legitimate purpose.
    ii. transactions which exceed the thresholds prescribed for specific categories of accounts.
    iii. transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer.
    iv. high account turnover inconsistent with the size of the balance maintained.

c. Bank will put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorization of customers will be carried out at a periodicity of not less than once in six months.
d. Bank will closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies. Branches will analyze data in cases where a large number of cheque books are sought by the company, there are multiple small deposits (generally in cash) across the country in one bank account and where a large number of cheques are issued bearing similar amounts/dates. Where such features are noticed by the branches and in case they find such unusual operations in their accounts, the matter will be immediately reported to Reserve Bank and other appropriate authorities such as FIU-IND.
e. Bank staff will keep a vigil over the transactions involving huge amounts. Transactions will generally have a bearing with the occupation and /or line of business of the account holders. In case of any doubt necessary enquiries be made with the account holders.
f. While accepting the cheque for collection, it is to be ensured that the name mentioned in the challan and name of the beneficiary of the instrument are same.
g. Bank will mandatorily obtain either PAN or Form 60 (if PAN is not available) for opening of accounts and also at the time of accepting cash receipt for Rs.50,000/- and above. If the customer appears to be structuring the transactions into a serious of transactions below the threshold of Rs.50,000/-, branches are required to obtain PAN or Form 60 (if PAN is not available) from the customer.
h. The Bank staff will maintain the standards of good conduct and behavior expected of them and not to involve in any activity that will bring disrepute to the institution and not to advise potential customers on the lines that will be an infringement of the legal process/ could facilitate money laundering/ could defeat the KYC norms or the norms of due diligence prescribed by RBI from time to time.

3.4.5 Risk Management

3.4.5.1 The inadequacy or absence of KYC standards can subject the Bank to serious customer and counter party risks especially reputational, operational, legal and financial risks.

Reputational Risk is defined as the potential that adverse publicity regarding the Bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution.

Operational Risk can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events.

Legal Risk is the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of the Bank.

Financial Risk is defined as the risk of loss arising due to any of the above risks or combination thereof resulting into the negative financial impact on the Bank.

In addition, the Bank will ensure the following for effectively implementing the AML/CFT requirements:

i. Using a risk-based approach to address management and mitigation of various AML/CFT risks.
ii. Allocation of responsibility for effective implementation of policies and procedures.
iii. Independent evaluation by the compliance functions of Bank's policies and procedures, including legal and regulatory requirements.
iv. Concurrent/ internal audit to verify the compliance with KYC/AML policies and procedures.
v. Putting up consolidated note on such audits and compliance to the Audit Committee at quarterly intervals.

Bank will prepare a profile for each new customer based on risk categorization. The customer profile can contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the bank.

Bank will categorize its customers into low, medium and high risk category based on the assessment and risk perception of the customers, identifying transactions that fall outside the regular pattern of activity and not merely based on any group or class they belong to.

Individuals (other than High Net Worth) and entities, whose identity and source of income, can be easily identified, and customers in whose accounts the transactions conform to the known profile, will be categorized as low risk. Illustrative examples include salaried employees and pensioners, people belonging to lower economic strata, government departments and government owned companies, regulators and statutory bodies, etc.

Customers who are likely to pose a higher than average risk will be categorized as medium or high risk depending on the background, nature and location of activity, country of origin, sources of funds, customer profile, etc. Customers requiring very high level of monitoring, e.g., those involved in cash intensive business, Politically Exposed Persons (PEPs) of foreign origin, will be categorized as high risk.

Whenever there are suspicions of money laundering or financing of activities relating to terrorism or where there are doubts about the veracity of previously obtained customer identification data, branches will review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of business relationship.

The above guidelines for risk categorization are indicative and operating officials can use their own judgement in arriving at the categorization for each account based on their own assessment and risk perception of the customers and not merely based on any group or class they belong to. Operating officials can also use for guidance in their own risk assessment, the reports and guidance notes on KYC/AML issued by the Indian Banks Association and RBI from time to time.

3.4.5.2 Review of Customer Risk Category:

Risk category of a customer is dynamic and is required to be reviewed.
Periodical Review: As per RBI Guidelines, Customer Risk Category is required to be reviewed periodically, at least at every six months essentially based on the transactions of the customer.

Event Based Review: Besides, as per various KYC/AML Guidelines it is necessary to undertake further/ enhanced due diligence, and review customer profiles if at any time during the relationship doubt arises about a customer's identity or activity, or about any transaction(s) carried out by the customer. In case of any such event, the customer's risk category also needs to be reviewed and moved to a higher category, if considered appropriate. Some of the triggers that will require review of customer risk category and movement to a higher risk category are given below.

a) Demographic Details: Shifting to high risk country, change in occupation of high risk nature, etc.
b) Account Status: Active, Inoperative, Dormant.
c) Account Vintage: less than six months old, etc.
d) Presence in Regulatory Negative/ PEP/ Defaulter/ Fraudster Lists
e) Transactions: Sudden spurt, Unusual transactions, Complex transactions, AML Alerts, etc.
f) Suspicious Transaction Report (STR) filed for the customer
g) The Bank will have appropriate system for periodical transaction based review of risk category, and also a mechanism for trigger based change in risk category.

3.4.5.3 Risk Categorization of Customer

i. Customers will be categorized into following risk categories:

Level I	**Low Risk**
Level II	**Medium Risk**
Level III	**High Risk**

Also, certain types of high-risk customers, like Politically Exposed Persons, carrying relatively higher degree of risk will be distinguished. The Bank can categorize the customers into very high risk where considered appropriate. The broad approach that will be followed in risk categorization is given in the following paragraphs

ii. Parameters for Risk Categorization

Customer Profile Characteristics - Following will be broad parameters to be adopted for customers in different risk categories initially:

Entity Parameters	Geographic	Financial Parameters	Activity Parameters	Linkage Parameters	Relationship Parameters
Constitution	Country of Residence	Financial status	Occupation	Source of Funds	Bank Accounts held
	Country of Origin				
Customers Background	Country of Incorporation	Expected Annual Income	Profession	Mode of Payments	Banking Services Availed
Social Status	Location of Customer	Expected Annual Turnover in the Account	Employment		Para Banking Services Availed
	Location of Customer Clients	Expected Annual Value of Other Services	Business Activity		

3.4.5.4 Product and Service/ New Technology Risk

Determining the potential Money Laundering and Terrorist Financing risks presented by services offered by a Bank or financial institution also assists in the overall risk assessment. The Bank will also factor in the services that pose a higher risk of ML / TF in determination of the overall risks.

Banking industry is continuously witnessing introduction of technology based new products with the evolution of Information and Communication Technology., the Bank will pay attention to any money laundering threats that can arise from new or developing technologies including internet banking that might favor anonymity, variety of Electronic Cards, mobile banking, etc. and take measures, where needed, to prevent their use in money laundering schemes.

The Bank will also be alert about the new or innovative services not specifically being offered by it, but that make use of the Bank's services to deliver the product.

In respect of various types of electronic cards that can be used for buying goods and services, drawing cash from ATMs, Electronic transfer of funds measures for prevention of Money Laundering will be adopted. The Bank will adopt all KYC/ AML/ CFT guidelines issued from time to time in respect of add-on/ supplementary cardholders also.

The Bank will ensure that appropriate KYC procedures will be duly applied before issuing the cards to the customers even where these are marketed through agents. The agents will also be subjected to KYC measures.

The Bank will factor in the higher risk while designing its products and processes with a view to build in suitable control mechanisms.

3.4.5.5 Geographic Risk

One of the factors in determining the risk is the location of the customer's business activity. The Bank will assess and pay special attention to the ML and FT risks of customers located in, and transactions from, other countries, including high-risk countries that do not or insufficiently apply the FATF Recommendations.

The Bank will therefore take into account risks arising from the deficiencies in AML/ CFT regime in the jurisdictions that are included in the FATF Statements issued periodically, and also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations.

Besides, the above certain other parameters that will be used for determining risk arising from a jurisdiction will be where existence/ effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, countries active in narcotics production, countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, countries against which government sanctions are applied, countries reputed to be any of the following - Havens/ sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent.

The Bank will also take into account the policies of various countries imposing restrictions/ sanctions over transactions with certain countries for various reasons, the policy of Government of India in dealing with these countries and other aspects while determining its approach to handling transactions with such countries.

The list of high / medium risk jurisdictions and locations will be subject to periodic revision based on the FATF lists of non-cooperative or deficient jurisdictions, advisories of UN, FIU-IND Guidelines, RBI guidelines, or media reports having any bearing on the risk perception.

A customer will be subject to higher due diligence if any of the following criteria falls under 'high risk' geographies:

a. Nationality (Individuals)
b. Residential address (Individuals)
c. Place of incorporation (Legal entities)
d. Residence of principal shareholders / beneficial owners (Legal entities) (e) Place of business registration such as branch / liaison / project office
e. Source of funds
f. Business or correspondence address
g. Country with whom customer deals (e.g. over 50% of business - trade, etc.)

3.4.5.6 Risk Management and Mitigation Measures

The Bank will have controls and procedures, approved by Senior management, to manage and mitigate effectively the identified risks, in line with the legal provisions and regulatory guidelines in this regard. The Bank will differentiate the extent of control measures, depending on the type and level of risk for the various risk factors. There will also be mechanisms to monitor the implementation of those controls and to enhance them.

Report of the IBA Working Group on Parameters for Risk Based Transaction Monitoring of March 2011 contains detailed guidelines on risk assessment and modalities of transaction monitoring. The indicative list of customers with potentially high ML / TF risk is given in the guidelines. Risk category of a customer is a function of numerous parameters, and the impact of any parameter on the risk posed by the customer will vary depending on the particular customer's situation. However, some basic principles will largely apply, and hence are useful in determining at least the initial risk category of a customer. It can be understood clearly that while applying these broad principles, any peculiar feature observed in respect of a specific customer will be duly considered, and the risk category accordingly decided. Further, the initial risk category can need to be reviewed or altered in the context of the business experience and transactions monitoring of the customer

Broad principles of risk based approach in managing ML/ TF risks are as follows:

a. Basic Criteria – Following are the basic criteria of risk based approach.

   i. Lower Risk – For lower risks the Bank will adopt simplified measures to manage and mitigate those risks.
   ii. Higher Risk – For higher risks the Bank will adopt enhanced measures to manage and mitigate the risks.

b. Nature of Customer Due Diligence – The extent of Customer Due Diligence to be carried out will differ depending on the risk category of customers, as indicated below.

   i. Low Risk Customers – For such customers 'Basic Due Diligence' measures will suffice suitably modified depending on relative risk perception.
   ii. Medium/ High Risk Customers – Such customers will be subjected to 'Enhanced Due Diligence' measures based on the degree of risk perception. Within the customers in this category, intensive 'enhanced due diligence' will be done for relatively higher risk customers, for instance PEPs.

c. Transaction Monitoring – For effective monitoring of transactions on ongoing basis also risk-based approach will be adopted.

   i. Low Risk Customers – The accounts and transactions of customers in this category will be subjected to normal monitoring with the appropriate thresholds being set for certain select parameters.
   ii. Medium/ High Risk Customers – The parameters and thresholds for monitoring of transactions and accounts of the customers in higher risk categories will be more stringent and elaborate.

3.5 Miscellaneous

3.5.1 At par cheque facility availed by co-operative banks

Since the 'at par' cheque facility offered by commercial banks to co-operative banks is in the nature of correspondent banking arrangement, Bank will monitor and review such arrangements to assess the risks including credit risk and reputational risk arising therefrom.

For this purpose, Bank will retain the right to verify the records maintained by the client cooperative Banks/ societies for compliance with the extant instructions on KYC and AML under such arrangements. In this regard, Urban Cooperative Banks (UCBs) are advised to utilize the 'at par' cheque facility only for the following purposes:

a. For their own use.
b. For their account holders who are KYC complaint provided that all transactions of Rs.50, 000/- or more will be strictly by debit to the customer's account.
c. For walk-in customers against cash for less than Rs.50,000/- per individual.

In order to utilize the 'at par' cheque facility in the above manner, Bank will ensure that UCBs will maintain the following:

a. Records pertaining to issuance of 'at par' cheques covering inter alia applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheque.

b. Sufficient balances/drawing arrangements with the commercial Bank extending such facility for purpose of honoring such instruments.

UCBs will also ensure that all 'at par' cheques issued by them are crossed 'account payee' irrespective of the amount involved.

3.5.2 Operation of Bank Accounts & Money Mules

Money mules are individuals with bank accounts who are recruited by fraudsters to receive cheque deposit or wire transfer for the purpose of money laundering. "Money Mules" can be used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "money mules." In order to minimize the operations of such mule accounts, Bank will strictly adhere to the guidelines on opening of accounts and monitoring of transactions.

3.5.3 Simplified norms for Self Help Groups (SHGs)

In order to address the difficulties faced by Self Help Groups (SHGs) in complying with KYC norms while opening Savings Bank accounts and credit linking of their accounts, following simplified norms will be followed by the Bank:

a. CDD of all the members of SHGs will not be required while opening the Savings Bank account of the SHGs and CDD of all the office bearers will suffice.
b. As regards CDD at the time of credit linking of SHGs, CDD of the all members is necessary.

3.5.4 Walk-in Customers

In case of transactions carried out by a non-account based customer, that is a walk-in customer, where the amount of transaction is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address will be verified.

If the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50000/-, the Bank will verify identity and address of the customer and also file a Suspicious Transaction Report to FIU-IND, as applicable. The identity and address of the Walk-in customer will be verified by obtaining KYC documents and records are to be maintained/ updated in the system. Bank will also verify the identity of the customers for all international money transfer operations.

3.5.5 Issue of Demand Drafts, etc., for more than Rs.50,000/-

The Bank will ensure that any remittance of funds by way of Demand Draft, mail/telegraphic transfer or any other mode and issue of Travelers' cheques for value of Rs.50,000/- and above will be effected by debit to the customer's account or against cheques and not against cash payment.

Bank will not make payment of cheques/drafts/pay orders/banker's cheques if they are presented beyond the period of three months from the date of such instrument.

Further, the name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheque, etc., as an issuing bank.

3.5.6 Unique Customer Identification Code

Bank will ensure that customers do not have multiple identities within a Bank by introducing a unique identification code for each customer. UCIC will be allotted to all customers while entering into new relationships. UCIC will also be allotted to walk-in customers who have frequent transactions with the Bank.

3.6 Correspondent Banking

Correspondent Banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services can include cash / funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc. Bank will take the following precautions while entering into a correspondent banking relationship:

a. Bank will gather sufficient information to fully understand the nature of the business of the bank including information on management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the bank's home country.
b. Such relationships can be established only with the approval of the Board or by a committee headed by the MD, Head – Branch Banking / Inclusive Banking / Corporate Banking / MSME and Chief Risk Officer. As required by RBI guidelines all approvals by the Committee will be put up to the Board of Directors in their next meeting for post-facto approval.
c. The responsibilities of each bank with whom correspondent banking relationship is established will be clearly documented.
d. In the case of payable-through-accounts, Bank will satisfy that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them.
e. Bank will also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.
f. Bank will be cautious while continuing relationships with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of Financial Action Task Force (FATF) Recommendations.
g. Bank will ensure that its respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.
h. Bank will not enter into a correspondent relationship with a "shell bank" (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.
i. Bank will not permit its accounts to be used by shell banks.

3.7 Wire Transfer

Banks use wire transfers as an expeditious method for transferring funds between bank accounts. Wire transfers include transactions occurring within the national boundaries of a country or from one country to another. As wire transfers do not involve actual movement of currency, they are considered as a rapid and secure method for transferring value from one location to another.

a. The salient features of a wire transfer transaction are as under:
    i. Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. The originator and the beneficiary can be the same person.
    ii. Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institutions are located in different countries. It can include any chain of wire transfers that has at least one cross-border element.

iii. Domestic wire transfer means any wire transfer where the originator and receiver are located in the same country. It can also include a chain of wire transfers that takes place entirely within the borders of a single country even though the system used to effect the wire transfer can be located in another country.

iv. The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the bank to perform the wire transfer.

v. Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and / or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analyzing suspicious or unusual activity and disseminating it as necessary.

vi. The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits. Accordingly, Bank will ensure that all wire transfers are accompanied with information of originator as per the extant guidelines

b. Cross-border wire transfers

i. All cross-border wire transfers must be accompanied by accurate and meaningful originator information.

ii. Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included.

iii. Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they can be exempted from including full originator information, provided they include the originator's account number or unique reference number as stated above.

c. Domestic wire transfers

i. Information accompanying all domestic wire transfers of Rs.50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.

ii. If the Bank has reason to believe that a customer is intentionally structuring wire transfers to below Rs.50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the Bank will insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts will be made to establish his identity and Suspicious Transaction Report (STR) will be made to FIU-IND.

iii. When a credit or debit card is used to effect money transfer, necessary information as stated above will be included in the message.

Inter-Bank transfers and settlements where both the originator and beneficiary are banks or financial institutions are exempted from the above requirements.

The Bank will ensure that the wire transfers received by it for its clients contain the required information, and similarly ensure that the wire transfers transactions made by it at the request of its clients contain the required information.

d. Exemptions

Inter-bank transfers and settlements where both the originator and beneficiary are banks or financial institutions will be exempted from the above requirements.

e. Role of Ordering, Intermediary and Beneficiary Banks

i. Ordering Bank

An Ordering Bank is the one that originates a wire transfer as per the order placed by its customer. As Ordering Bank, the Bank will ensure that qualifying wire transfers contain complete originator information. The Bank will also verify and preserve the information at least for a period of five years.

ii. Intermediary Bank

For both cross-border and domestic wire transfers, Bank processing an intermediary element of a chain of wire transfers will ensure that all originator information accompanying a wire transfer is retained with the transfer. Where technical limitations prevent full originator information accompanying a cross border wire transfer from remaining with a related domestic wire transfer, a record will be kept at least for five years (as required under Prevention of Money Laundering Act, 2002) as the receiving Intermediary Bank of all the information received from the Ordering Bank.

iii. Beneficiary Bank

A Beneficiary Bank will have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information can be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they will be reported to the Financial Intelligence Unit-India. As Beneficiary Bank, the Bank will also take up the matter with the Ordering Bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information on the remitter, the Bank will consider restricting or even terminating its business relationship with the Ordering Bank.

3.8 Records Management

PML Act and Rules cast certain obligations on the banks with regard to maintenance, preservation and reporting of customer account information. Bank will take all steps considered necessary to ensure compliance with the requirements of the Act and Rules ibid and RBI regulations.

3.8.1 Maintenance of records of transactions

Nature of Records to be maintained:

i. All series of cash transactions integrally connected to each other which have been valued below Rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees ten lakhs.
ii. All cash transactions of the value of more than Rupees ten lakhs or its equivalent in foreign currency
iii. All transactions involving receipts by non-profit organizations of value more than Rupees ten lakhs or its equivalent in foreign currency
iv. All cash transactions where forged or counterfeit currency notes or Bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transaction and
v. All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.
vi. All cross border transactions valuing Rupees five lakhs or more.

vii. Identity documents (including updated records of identification data) of the customers and the beneficial owners as well as account files and business.

3.8.2 Information to be on Record

Transaction Records maintained will contain the following information:

i. Nature of the transaction;
ii. Amount of the transaction and the currency in which it was denominated;
iii. Date on which the transaction was conducted; and
iv. Parties to the transaction

3.8.3 Preservation of Records

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

i. Bank will maintain for at least five years from the date of transaction between the Bank and the customers, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

ii. Bank will ensure that records pertaining to the identification of the customers and their address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended. The identification records and transaction data will be made available to the competent authorities upon request.

iii. Bank will maintain records of the identity of clients, and records in respect of transactions with its clients , in hard or soft format.

iv. Bank will pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background, including all documents / office records / memorandums pertaining to such transactions and purpose thereof will, as far as possible, be examined and the findings, at branch as well as Principal Officer level, will be properly recorded. Such records and related documents will be made available to help auditors to scrutinize the transactions and also to Reserve Bank / other relevant authorities. These records will be preserved for five years as is required under PMLA, 2002.

v. Preservation of records will also be governed by the 'Record Retention' policy of the Bank approved by the Board from time to time.

3.9 Combating Financing of Terrorism

3.9.1 United Nations Security Council Resolutions

The United Nations periodically circulates the following two lists of individuals and entities, suspected of having terrorist links, and as approved by its Security Council (UNSC):

a. The ISIL (Da'esh) & Al-Qaida Sanctions List includes names of individuals, groups, undertakings and entities associated with the ISIL (Da'esh) /Al-Qaida. The updated ISIL (Da'esh) /Al-Qaida Sanctions List is available at http:// www.un.org/ sc/ committees/ 1267/ aq_sanctions_list.shtml.

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 http://www.un.org/sc/committees/1988/list.shtml.

The Bank will screen customer names with UN List of terrorist individuals/entities before creation of new customer ID/opening of accounts. The Bank will ensure that names/s of the proposed customer does not match with that of the UN list of Terrorist individuals/organization/ entities, before opening any new account.

The Bank is also required to cross check the details of all existing accounts with the updated list and ensure that no account is held by or linked to any of the entities or individuals included in the list maintained for this purpose. If the particulars of any of the account/s have resemblance with those appearing in the list, the Bank will verify transactions carried out in such accounts and report those accounts to RBI/Financial Intelligence Unit-INDIA, New Delhi.

3.9.2 Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) -Implementation

These lists are required are to be taken into account for the purpose of implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA).

Sec. 51A. For the prevention of, and for coping with Terrorist activities, the Central Government will have power to –

a. freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;
b. prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism;
c. prevent the entry into or the transit through India of individuals Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism

Pursuant to these requirements the Bank will take the following measures:

a. Before opening any new account: To ensure that the name of the proposed customer does not appear in the said lists.
b. On revision of the Lists: To scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the lists.

c. On an account holder resembling with any entity/ individual in the said lists: To immediately intimate full details of such accounts to RBI and FIUIND. In case of Demat accounts the details of such entity/ individual will be advised to SEBI and FIU-IND.

3.10 Reporting Requirements to FIU

a. Reporting to Financial Intelligence Unit –India

The Bank is obliged, in terms of the Rule 3 of the PML (Maintenance of Records) Rules, 2005, to furnish information relating to cash transactions, Cash transactions integrally connected to each other, and all transactions involving receipts by non-profit organizations (NPO means any entity or organization that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered (erstwhile Section 25 of Companies Act, 1956) under Section 8 of the Companies Act, 2013), Cash transactions were forged or counterfeit currency notes or Bank notes have been used as genuine, Cross border wire transfer, etc. to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri,
New Delhi-110021
Website - http://fiuindia.gov.in/

b. Reports to be furnished to FIU-IND

i. Cash Transaction Report (CTR)

While detailed instructions for filing all types of reports are given in the instructions part of the related formats, Bank will scrupulously adhere to the following:

1. The CTR for each month will be submitted to FIU-IND by 15th of the succeeding month. Cash transaction reporting by branches to their controlling offices will, therefore, invariably be submitted on monthly basis and Bank will ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.
2. While filing CTR, details of individual transactions below Rupees Fifty thousand need not be furnished.
3. CTR will contain only the transactions carried out by the Bank on behalf of their clients/customers excluding transactions between the internal accounts of the Bank.
4. A summary of cash transaction reports for the Bank as a whole will be compiled by the Principal Officer of the Bank every month in physical form as per the format specified. The summary will be signed by the Principal Officer and submitted to FIU-IND. In case of CTRs compiled centrally by banks for the branches having Core Banking Solution (CBS) at their central data center, banks can generate centralized CTRs in respect of the branches under core banking solution at one point for onward transmission to FIU-IND, provided the CTR is to be generated in the format prescribed by FIU-IND;
5. A copy of the monthly CTR submitted to FIU-India in respect of the branches will be available at the branches for production to auditors/inspectors, when asked for; and
6. However, in respect of branches not under CBS, the monthly CTR will continue to be compiled and forwarded by the branch to the Principal Officer for onward transmission to FIU-IND.

ii. Counterfeit Currency Report (CCR):

All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine will be reported by the Principal Officer of the Bank to FIU-IND in the specified format(Counterfeit Currency Report – CCR), by 15thday of the next month. These cash transactions will also include transactions where forgery of valuable security or documents has taken place and can be reported to FIU-IND in plain text form.

iii. Suspicious Transaction Reports (STR)

While determining suspicious transactions, Bank will be guided by the definition of suspicious transaction as contained in PMLA Rules as amended from time to time.

1. It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. Bank will report all such attempted transactions in STRs, even if not completed by the customers, irrespective of the amount of the transaction, as per extant instructions.
2. Bank will make STRs if they have reasonable ground to believe that the transaction involves proceeds of crime irrespective of the amount of the transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.
3. The STR will be furnished within seven days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer will record his reasons for treating any transaction or a series of transactions as suspicious. It will 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. Such report will be made available to the competent authorities on request.
4. In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, Banks can consider the indicative list of suspicious activities contained in 'IBA's Guidance Note for Banks, January 2012'.
5. Bank will not put any restrictions on operations in the accounts where an STR has been filed. Bank (and employees) will keep the fact of furnishing of STR strictly confidential, as required under PML Rules. It will be ensured that there is no tipping off to the customer at any level.

iv. Non-Profit Organization

The report of all transactions involving receipts by non- profit organizations of value more than Rupees ten lakhs or its equivalent in foreign currency will be submitted every month to the Director, FIU-IND by 15th of the succeeding month in the prescribed format.

v. Cross-border Wire Transfer

Cross-border Wire Transfer Report (CWTR) is required to be filed with FIU-IND by 15th of succeeding month for all cross border wire transfers of the value of more than Rupees five lakhs or its equivalent in foreign currency where either the origin or destination of fund is in India.

3.11 General Guidelines

3.11.1 Confidentiality of customer information

The information collected from the customer for the purpose of opening of account will be treated as confidential and details thereof will not be divulged for the purpose of cross selling etc. Information sought from the customer

will be relevant to the perceived risk and be non-intrusive. Any other information that is sought from the customer will be called for separately only after the account has been opened, with his/her express consent and in a different form, distinctly separate from the application form. It will be indicated clearly to the customer that providing such information is optional.

3.11.2 Secrecy Obligations and Sharing of Information

Bank will maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.

Information collected from customers for the purpose of opening of account will be treated as confidential and details thereof will not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.
While considering the requests for data/ information from Government and other agencies, Bank 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. The exceptions to the said rule will 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 Bank requires disclosure and
d. Where the disclosure is made with the express or implied consent of the customer.

3.11.3 Avoiding hardship to customers

While issuing operational instructions to branches, Bank will keep in mind the spirit of the instructions issued by the Reserve Bank so as to avoid undue hardships to individuals who are otherwise classified as low risk customers.

3.11.4 Sensitizing Customers

Implementation of AML/CFT policy can require certain information from customers of a personal nature or which had not been called for earlier. The purpose of collecting such information could be questioned by the customer and can often lead to avoidable complaints and litigation. Bank will; therefore, prepare specific literature / pamphlets etc. to educate the customer regarding the objectives of the AML/CFT requirements for which their cooperation is solicited.

3.11.5 Hiring of Employees

KYC norms / AML standards / CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking channels. Therefore, Bank will put in place adequate screening mechanism as an integral part of its personnel recruitment / hiring process.

3.11.6 Employee Training

Bank will have an ongoing employee-training programme so that the members of the 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 needs to 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 the Bank, regulation and related issues will be ensured.

3.11.7 Accounts under Foreign Contribution Regulation Act, 2010 (FCRA)

In terms of the Foreign Contribution Regulation Act, 2010, certain categories of individuals and organizations are required to obtain prior permission from the Central Government (Secretary, Ministry of Home Affairs, GOI, New Delhi) to receive "Foreign Contributions" or accept "Foreign Hospitality" and such receipts/acceptance require reporting to the Government.

a. Individuals/Organizations who cannot receive foreign contributions:

Foreign contributions cannot be accepted by candidate for election, correspondent, columnist, cartoonist, editor, owner, printer or publisher of a registered newspaper, judge, Government servant or employee of any corporation, member of any legislature, political party or office bearer thereof.

b. Individuals/Organizations who can receive foreign contributions:

An association having a definite cultural, economic, educational, religious or social programme can receive foreign contribution after it obtains the prior permission of the Central Government or gets itself registered with the Central Government.

Bank will ensure that the provisions of the Foreign Contribution (Regulation) Act, 2010, wherever applicable, are strictly adhered to.

3.11.8 Applicability to overseas branches/subsidiaries

The guidelines in this circular apply to the branches and majority owned subsidiaries located abroad, to the extent local laws in the host country permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same will be brought to the notice of the Reserve Bank. In case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of Banks are required to adopt the more stringent regulation of the two.

3.11.9 Technology requirements

The AML software in use at Bank needs to be comprehensive and robust enough to capture all cash and other transactions, including those relating to walk-in customers, sale of gold/silver/platinum, payment of dues of credit cards/reloading of prepaid/travel cards, third party products, and transactions involving internal accounts of the Bank.

3.11.10 Principal Officer

Bank can appoint a senior officer from compliance department as Principal Officer (PO). The PO will be independent and report directly to the senior management. The PO will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. The name, designation and address of the Principal Officer can be communicated to the FIU-IND.

The role and responsibilities of the Principal Officer include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of money Laundering Act, 2002, rules and regulations made there under, as amended from time to time.

The Principal Officer is responsible for timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency to FIU-IND. The Principal Officer and other appropriate staff will have timely access to customer identification data and other CDD information, transaction records and other relevant information.

3.11.11 Quoting of PAN

Permanent account number (PAN) or equivalent e-document thereof of customers will be obtained and verified while establishing an account based relationship and undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time. Form 60 will be obtained from persons who do not have PAN) or equivalent e-document thereof. PAN is mandatory certain category of customers (Refer Annexure I).

3.11.12 Selling Third Party Products

Bank, acting as agent while selling third party products as per regulations in force from time to time, will comply with the following aspects:

a. the identity and address of the walk-in customer will be verified for transactions above rupees fifty thousand as required under Section 13(e) of the Master Direction - Know Your Customer (KYC) Direction, 2016.
b. transaction details of sale of third party products and related records will be maintained.
c. AML software capable of capturing, generating and analyzing alerts for the purpose of filing CTR / STR in respect of transactions relating to third party products with customers including walk-in customers will be available.
d. Sale of third party products by the Bank as agents to customers, including walk-in customers, for Rs.50,000 and above must be by

    i. debit to customer's account or against cheques and
    ii. obtaining& verification of the PAN given by the account based as well as walk-in customers.

e. This instruction at 'd' above, will also apply to sale of Bank's own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for Rs.50, 000/- and above.

3.11.13 Introduction of New technologies

Bank will pay special attention to the money laundering and terrorist financing threats arising from new or developing technologies and take necessary steps to prevent its misuse for money laundering and terrorist financing activities. Bank will ensure that appropriate KYC / AML & CFT Procedures are duly applied to the customers using the new technology driven products.

3.11.14 Report to the Board

Instances of AML/KYC incidents will be reported to the Board of Directors at quarterly intervals. However, occurrence of incidents, if any, of serious nature will be reported to the Board immediately in the next Board meeting.

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

Central KYC Records Registry" (CKYCR) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer. In terms of provision of Rule 9(1A) of PML Rules, the Bank shall capture customer's KYC records and upload onto CKYCR within the prescribed time and as per the extant guidelines.

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

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

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

(iii) the Bank 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.

3.12 Money Laundering and Terrorist Financing Risk Assessment.

Bank 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 Bank will take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may from time to time. The risk assessment will submitted to the Board on an annual basis.

4 Provisions in policy over and above but in consonance with RBI guidelines

The above policy is in consonance with the RBI regulations.

5 Changes to the Policy

a) Regulatory changes in line with Master Directions on Prepaid Payment Instruments (PPIs) dated August 27, 2021 introduced at 2.2 and 3.4.2.6.

6 Periodicity of Review of the Policy

The Board will review this policy at annual intervals and at such intervals as will be required on the regulatory and business exigencies.

Author of the Policy	**Compliance**
Name of Committee which recommended to the Board	**Executive Policy Formulation Committee**
Date of Board Approval	28-01-22
Date of Next Review	28-01-23

Annexure I

Customer Identification Procedure

Documents to be obtained from customers

Types of Customers	Description of Documents Certified copy of any One of the following Officially Valid Documents (OVDs). [Copy verified from the Originals will be kept on record with AOF].
Accounts of Individuals Proof of Identity and Address	1. Passport 2. Driving Licence 3.proof of possession of Aadhaar number* 4. Voter's Identity Card issued by the Election Commission of India 5. Job card issued by NREGA duly signed by an officer of the State Government. 6.Letter issued by the National Population Register containing details of name, address, or any other document as notified by the Central Government in consultation with the Regulator. And 7. The Permanent Account Number or Form No. 60 as defined in Income-tax Rules, 1962, * The manner in which Aadhaar to be obtained and authenticated shall be covered extensively in the process note.
Accounts of Companies	(i) Certificate of incorporation; (ii) Memorandum and Articles of Association; (iii) Permanent Account Number of the Company (iv) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; (v) Officially Valid Document (b) Permanent Account Numbers or Form 60 as defined in the Income-tax Rules, 1962, issued to managers, officers or employees holding an attorney to transact on the company's behalf
Accounts of Partnership firms	(i) registration certificate; (ii) partnership deed; (iii) Permanent Account Number of the Partnership Firm (iv) (a) Officially Valid Document (b) Permanent Account Number or Form 60 as defined in the Income-tax Rules, 1962, issued to the person holding an attorney to transact on its behalf
Accounts of Proprietorship concerns - Proof of the name, address and activity of the concern	Apart from customer identification procedure as applicable to the proprietor any two of the following documents in the name of the proprietary concern would suffice: (i) Registration certificate (in the case of a registered concern) (ii) Certificate / licence issued by the Municipal authorities under Shop & Establishment Act, (iii) Sales and income tax returns (iv) CST / VAT / GST certificate (provisional/final)

	(v) Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities (vi) Licence / certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. (vii) The complete Income Tax return (not just the acknowledgement) in the name of the sole Proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax Authorities. (viii) Importer Exporter Code (IEC) issued to the Proprietary concern by the office of DGFT/Licence/Certificate of practice issued in the name of the Proprietary concern by any professional body incorporated under a statute. Note: However, in cases where the Bank is satisfied that it is not possible to furnish two such documents in the name of proprietary concern, the Bank will accept only one of the above mentioned documents as activity proof provided that the Bank undertakes contact point verification, collects such information as is required to establish the existence of such firm, confirms, clarifies and satisfies itself that the business activity is verified from the address of the proprietary concern.
Accounts of trusts	(i) registration certificate; (ii) trust deed; (iii) Permanent Account Number or Form 60 of the Trust (iv) (a) Officially Valid Document (b) Permanent Account Number or Form 60 as defined in the Income-tax Rules, 1962, issued to the person holding an attorney to transact on its behalf .
Accounts of unincorporated association or a body of individuals	(i) resolution of the managing body of such association or body of individuals; (ii) power of attorney granted to him to transact on its behalf; (iii) Permanent Account Number or Form 60 of the Trust (iv) (a) Officially Valid Document; and (b) Permanent Account Number or Form 60 as defined in the Income-tax Rules, 1962, issued to the person holding, an attorney to transact on its behalf
Accounts of Hindu Undivided Family	In addition to KYC documents of Karta and Major Coparceners, the following documents should be obtained: Declaration of HUF and its Karta Recent Passport Photographs duly self-attested by Karta and major co-parceners. Names and addresses of Karta and Major Coparceners. An officially valid document in respect of the person holding an attorney to transact on its behalf.
Accounts of Government or its Departments, Societies, Universities and Local Bodies like Village Panchayats:	Document showing name of the person authorized to act on behalf of the entity; Officially Valid Documents for proof of identity and address in respect of the person holding a power of attorney to transact on its behalf and Such documents as may be required by the Bank to establish the legal existence of such an entity/ juridical person

Annexure II

List of High / Medium/ Low risk Customers based on the recommendations of IBA Working Group.		
High Risk	**Medium Risk**	**Low Risk**
1. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc. 2. Individuals or entities listed in the schedule to the order under Section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities 3. Individuals and entities in watch lists issued by Interpol and other similar international organizations 4. Customers with dubious reputation as per public information available or commercially available watch lists 5. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk 6.Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the Customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations etc. 7.Customers based in high risk countries/jurisdictions or locations 8. Politically exposed persons (PEPs) of foreign origin, Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner; 9.Non-resident Customers and foreign nationals 10. Embassies / Consulates 11. Off-shore (foreign) corporation/ business 12. Non face-to-face Customers 13. High net worth individuals 14. Firms with 'sleeping partners' 15. Companies having close family shareholding or beneficial ownership 16. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale 17. Shell companies, which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence 18.Investment Management / Money Management Company/Personal Investment Company	1. Gas Station 2.Car / Boat / Plane Dealership 3. Electronics (wholesale) 4. Travel agency 5. Used car sales 6. Telemarketers 7.Providers of telecommunications service, internet café, IDD call service, phone cards, phone centre 8. Dot-com company or internet business 9. Pawnshops 10. Auctioneers 11. Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theatres, etc. 12. Sole Practitioners or Law Firms (small, little known) 13.Notaries (small, little known) 14. Secretarial Firms (small, little known) 15. Accountants (small, little known firms) 16.Venture capital companies 17. Blind 18. Purdanashin. 19. Registered Body. 20. Corporate Body 21. Joint Sector 22. Partnership 23. Private Bank 24. Private Limited Company 25. Unregistered body. 26. Proprietorship.	1. Cooperative Bank 2. Ex-staff, Govt./ Semi Govt. Employees 3. Illiterate 4. Individual 5. Local Authority 6. Other Banks 7. Pensioner 8. Public Ltd. 9. Public Sector 10. Public Sector Bank 11. Staff. 12. Regional Rural Banks 13.Govt./Semi- Govt. Local Body 14. Cooperative Society 15. Senior Citizens 16. Self Help Groups

19. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc. 20.Trusts, charities, NGOs/NPOs (especially those operating on a "cross-border" basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies) 21. Money Service Business: including seller of: Money Orders / Travellers' Cheques / Money Transmission / Cheque Cashing / Currency Dealing or Exchange 22.Business accepting third party cheques (except supermarkets or retail stores that accept payroll cheques/cash payroll cheques) 23.Gambling/gaming including "Junket Operators" arranging gambling tours 24.Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers). 25. Customers engaged in a business, which is associated with higher levels of corruption (e.g., Arms manufacturers, dealers and intermediaries). 26. Customers engaged in industries that might relate to nuclear proliferation activities or explosives. 27. Customers that may appear to be Multi-level marketing companies etc. 28. Customers dealing in Real Estate business (transactions need to be monitored with enhanced due diligence). 29. Associations/Clubs 30. Foreign Nationals. 31. NGO. 32. Overseas Corporate Bodies. 33. Bullion dealers and Jewellers (subject to enhanced due diligence) 34. Pooled accounts. 35. Other Cash Intensive business. 36. Shell Banks – Transactions in corresponding banking. 37. Non-Bank Financial Institution 38. Stock brokerage 39. Import / Export 40. Executors/Administrators 41. HUF. 42. Minor. 43. Accounts under Foreign Contribution Regulation Act.		