SAURASHTRA GRAMIN BANK

KNOW YOUR CUSTOMER (KYC) POLICY

1. INTRODUCTION

In order to prevent banks and other financial institutions from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system, efforts are continuously being made both internationally and nationally, by way of prescribing various rules and regulations. Internationally, the Financial Action Task Force (FATF) which is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions, sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. As our country is a member of FATF, we are committed to upholding measures to protect the integrity of international financial system.

In India, the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, form the legal framework on Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT). In terms of the provisions of the PML Act, 2002 and the PML Rules, 2005, as amended from time to time by the Government of India, Bank is required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions.

Accordingly, in exercise of the powers conferred by Sections 35A of the Banking Regulation Act, 1949, the Banking Regulation Act (AACS), 1949, read with Section 56 of the Act ibid, Sections 45JA, 45K and 45L of the Reserve Bank of India Act, 1934, Section 10 (2) read with Section 18 of Payment and Settlement Systems Act 2007 (Act 51 of 2007), Section 11(1) of the Foreign Exchange Management Act, 1999, Rule 9(14) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 and all other laws enabling the Reserve Bank in this regard, the Reserve Bank of India issues KYC directions in public interest which we cover in this KYC policy.

This renewal policy document has been prepared in line with the RBI guidelines vide Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated 25/02/2016 **(updated as on May 04, 2023)** /NABARD guidelines and incorporates the Bank's approach to KYC, AML and CFT issues.

CHAPTER – I

PRELIMINARY

2. OBJECTIVE, SCOPE AND APPLICATION OF THE POLICY

The primary objective of the policy is to prevent the Bank from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. Purposes proposed to be served by the policy are:

a) To prevent criminal elements from using the Bank for money laundering activities

b) To enable the Bank to know/ understand the customers and their financial dealings better which, in turn, would help the bank to manage risks prudently

c) To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.

d) To comply with applicable laws and regulatory guidelines.

e) To ensure that the concerned staffs are adequately trained in KYC/ AML/ CFT procedures.

f) To establish procedures for verification of identification of individuals / non-individuals for opening of account.

This Policy is applicable to all branches/offices of the Saurashtra Gramin Bank and is to be read in conjunction with related operational guidelines issued from time to time. While bank will apply

KYC-AML-CFT norms, standards and procedures prescribed by NABARD/RBI/Other regulatory agency in this policy to all prospective / new customers, the same would also be applied to all existing customers without any exception. These guidelines shall also be applicable to all digital Banking Services offered by the Bank.
Provided that this rule will not apply to 'small accounts' referring to Section 18 of this policy.

3. DEFINITIONS

In this Policy, unless the context otherwise requires, the terms herein will bear the meanings assigned to them below:
(a) Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:

i. "**Aadhaar number**" will have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);

ii. "**Act**" and "**Rules**" means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

iii. "Authentication", in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) +`Act, 2016.

iv. **Beneficial Owner (BO)**

a. Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.

1. "Controlling ownership interest" means ownership of/entitlement to more than 10 percent of the 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.

b. Where the customer 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/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.

c. Where the customer 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/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d. Where the customer is a trust, the identification of beneficial owner(s) will include identification of the author of the trust, the trustee, the beneficiaries with 10 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.

v. "Certified Copy" - Obtaining a certified copy by the Bank will mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the BANK as per the provisions contained in the Act.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, may be obtained:
• Authorised officials of overseas branches of Scheduled Commercial Banks registered in India, • Branches of overseas banks with whom Indian banks have relationships,
• Notary Public abroad,
• Court Magistrate,
• Judge,
• Indian Embassy/Consulate General in the country where the non-resident customer resides.

vi. "**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.

vii. "Designated Director" means a person designated by the Bank to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules. A person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Regional Rural Banks.

viii. "Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Bank as per the provisions contained in the Act.

ix. "Digital Signature" will have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

x. "Equivalent e-document" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

xi. **"Group"** – The term "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act, 1961. (43 of 1961).

xii. "Know Your Client (KYC) Identifier" means the unique number or code assigned to a customer by the Central KYC Records Registry.

xiii. "Non-profit organisations" (NPO) means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), 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 (18 of 2013).

xiv. "Officially Valid Document" (OVD) means the passport, the driving licence, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that,

a. Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

b. Where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof will be deemed to be OVDs for the limited purpose of proof of address:-

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

ii. Property or Municipal tax receipt;

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

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

c. The customer will submit OVD with current address within a period of three months of submitting the documents specified at 'b' above

d. 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.

xv. "Offline verification" will have the same meaning as assigned to it in clause(pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

xvi. "Person" has the same meaning assigned in the Act and includes:

- **a.** An individual,
- **b.** A Hindu undivided family,
- **c.** A company,
- **d.** A firm,
- **e.** An association of persons or a body of individuals, whether incorporated or not,
- **f.** Every artificial juridical person, not falling within any one of the above persons (a to e),
- **g.** Any agency, office or branch owned or controlled by any of the above persons (a to f).

xvi. "Principal Officer" means an officer nominated by the Bank, responsible for furnishing information as per rule 8 of the Rules.

xvii. "Suspicious transaction" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

- **a.** Gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
- **b.** Appears to be made in circumstances of unusual or unjustified complexity; or
- **c.** Appears to not have economic rationale or bona-fide purpose; or
- **d.** Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

xviii. A **'Small Account'** means a savings account which is opened in terms of sub-rule (5) of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are specified in Section 18.

xix. "Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

a. Opening of an account;

b. Deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;

c. The use of a safety deposit box or any other form of safe deposit;

d. Entering into any fiduciary relationship;

e. Any payment made or received, in whole or in part, for any contractual or other legal obligation; or

f. Establishing or creating a legal person or legal arrangement.

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

(b) Terms bearing meaning assigned in this Policy, unless the context otherwise requires, will bear the meanings assigned to them below:

i. "Common Reporting Standards" (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

ii. "Customer" means a person who is engaged in a financial transaction or activity with Bank and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

iii. "Walk-in Customer" means a person who does not have an account-based relationship with the Bank, but undertakes transactions with the Bank.

iv. "Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner.

v. "Customer identification" means undertaking the process of CDD.

vi. "FATCA" means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

vii. "IGA" means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.

viii. "KYC Templates" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

ix. "Non-face-to-face customers" means customers who open accounts without visiting the branch/offices of the Bank or meeting the officials of Bank.

x. "On-going Due Diligence" means regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.

xi. "Periodic Updation" means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

xii. "Politically Exposed Persons" (PEPs) 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.

xiii. "Wire transfer" related definitions:

a. Batch transfer: Batch transfer is a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions but may/may not be ultimately intended for different persons.

b. Beneficiary: Beneficiary refers to a natural or legal person or legal arrangement who / which is identified by the originator as the receiver of the requested wire transfer.

c. Beneficiary Bank: It refers to a financial institution, regulated by the RBI, which receives the wire transfer from the ordering financial institution directly or through an intermediary Bank and makes the funds available to the beneficiary.

d. Cover Payment: Cover Payment refers to a wire transfer that combines a payment message sent directly by the ordering financial institution to the beneficiary financial institution with the routing of the funding instruction (the cover) from the ordering financial institution to the beneficiary financial institution through one or more intermediary financial institutions.

e. Domestic wire transfer: Domestic wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in India. This term, therefore, refers to any chain of wire transfer that takes place entirely within the borders of India, even though the system used to transfer the payment message may be located in another country.

f. Financial Institution: In the context of wire-transfer instructions, the term 'Financial Institution' shall have the same meaning as has been ascribed to it in the FATF Recommendations, as revised from time to time.

g. Intermediary Bank: Intermediary Bank refers to a financial institution or any other entity, regulated by the RBI which handles an intermediary element of the wire transfer, in a serial or cover payment chain and that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution.

h. Ordering Bank: Ordering Bank refers to the financial institution, regulated by the RBI, which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.

i. Originator: Originator refers to the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.

j. Serial Payment: Serial Payment refers to a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering financial institution to the beneficiary financial institution directly or through one or more intermediary financial institutions (e.g., correspondent banks).

k. Straight-through Processing: Straight-through processing refers to payment transactions that are conducted electronically without the need for manual intervention.

l. Unique transaction reference number: Unique transaction reference number refers to a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer.

m. Wire transfer: Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

(c) All other expressions unless defined herein will have the same meaning as have been assigned to them under the Banking Regulation Act,1949, the Reserve Bank of India Act,1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made there under, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

CHAPTER –II

General

4. The KYC policy will include following four key elements:

a) Customer Acceptance Policy;

b) Risk Management;

c) Customer Identification Procedures (CIP); and

d) Monitoring of Transactions

4A. Money Laundering and Terrorist Financing Risk Assessment by Bank:

(a) 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 assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, Bank will take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with Bank from time to time.

(b) For the purpose of Money Laundering Risk Categorization, Individuals (other than High Net Worth) and Entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, will be classified as Low Risk, subject to other parameters fixed by bank for categorizing such customers as Low Risk (Illustrative examples of low risk customers are salaried employees whose salary structures are well defined, pensioners, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc.) In case of Low Risk Customers, bank's policy will ensure that basic requirements of verifying the identity and location of the customer are met with.

Customers who are likely to pose higher than average Money Laundering Risk to the bank should be categorized as Medium or High Risk customers, depending on their background, nature and location of activity, country of origin, sources of funds, customer profile, annual Income / Turnover etc. Customers requiring high level of monitoring, e.g. those involving cash intensive business, politically exposed persons (PEPs) of foreign origin may, if considered, be categorized as High Risk. Tentative list attached as per Annex – 3

(c) The outcome of the exercise will be put up to the Board and should be available to competent authorities and self-regulating bodies.

(d) Whitelisting / Trusted Account for AML/CFT

Accounts eligible for white-listing/ Trusted Accounts are those of Government department/ undertaking, Schedule Bank, RRB, Co-Operative Bank, various funds managed/ regulated by the Government/ Quasi-Government bodies where the scope of suspicious transaction is almost NIL/ Negligible.

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

5. Designated Director:

(a) A "Designated Director" means a person designated by the Bank to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules thereof. Designated Director will be nominated by the Board. (General Manager (O) will act as Designated Director.)

(b) The name, designation and address of the Designated Director will be communicated to the FIU-IND.

(c) The name, designation, address and contact details of the Designated Director will be communicated to the RBI.

(d) In no case, the Principal Officer will be nominated as the 'Designated Director'.

6. Principal Officer:

(a) The Principal Officer will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. (The Head of Department (Audit) will be assigned the responsibilities of Principal Officer Who will be posted at the Head office of the Bank and will be responsible for monitoring and reporting of all transactions and sharing of information as required under the law.)

(b) The name, designation and address of the Principal Officer will be communicated to the FIU-IND.

(c) The name, designation, address and contact details of the Principal Officer will be communicated to the RBI.

(d) Principal Officer shall have below mentioned responsibilities:

i. Implementation of the bank's KYC-AML-CFT Policy in the bank.
ii. Sharing of information as required under the law.
iii. Maintaining close liaison with enforcement agencies, banks and any other institution which are involved in the fight against Money Laundering and Combating Financing of Terrorism (CFT)
iv. Ensuring submission of cash Transaction Report (CTR) to FIU-IND, New Delhi within 15 days of every succeeding month.
v. Ensuring submission of Suspicious Transaction Report (STR) to FIU-IND, New Delhi within seven days from the date of arriving at conclusion that transaction is suspicious.

vi. Ensuring submission of Non - Profit Organization Transaction Report (NTR) of value more than Rupees 10 lacks or its equivalent in foreign currency to FIU-IND, New Delhi within 15 days of every succeeding month.

vii. Ensuring Monthly Reporting of the CTRs / STRs / NTRs to FIU-IND, New Delhi and about implementation of KYC-AML-CFT policy in the bank to the Board on quarterly basis.

viii. Ensuring updation/ revision of KYC-AML-CFT policy of the bank by incorporating guidelines/ instructions issued by Reserve Bank of India from time to time.

ix. Ensuring compliance of Regulatory Guidelines / Instructions and obligation of bank under PML Act 2002.

7. Responsibilities of Regional Heads:

Regional Heads will:

a. Ensure Compliance of KYC-AML-CFT Policy / Guidelines of bank by all the branches under their control and supervision.

b. Consider observations of Internal Inspectors / Concurrent Auditors reported in their Inspection Reports on deficiency or non-compliance of guidelines on KYC-AML-CFT by any of the branches in the Region and ensure rectification thereof by their Branch Heads and will send their report to Principal Officer (PO) on monthly basis.

c. Sending confirmation on monthly basis to the Chief Compliance officer/Principal Officer for having complied fully with the KYC-AML-CFT guidelines of the bank in new as well old existing accounts.

d. Sending confirmation for completion of review process for Money Laundering Risk Categorization in the first week of the January and July to the Principal Officer to meet with the requirement of Regulators.

8. Compliance of KYC policy

(a) Bank will ensure compliance with KYC Policy through:

i. Specifying as to who constitute, 'Senior Management' for the purpose of KYC compliance.

ii. Allocation of responsibility for effective implementation of policies and procedures.

iii. Independent evaluation of the compliance functions of Banks' policies and procedures, including legal and regulatory requirements.

iv. Concurrent / internal audit system to verify the compliance with KYC/AML policies and procedures.

v. Submission of quarterly audit notes and compliance to the Audit Committee.

(b) Bank will ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

CHAPTER – III

Customer Acceptance Policy

9. Customer Acceptance Policy of the Bank will be as under.

10. Without prejudice to the generality of the aspect that Customer Acceptance Policy may contain, Bank will ensure that:

(a) No account is opened in anonymous or fictitious/benami name.

(b) No account is opened where the Bank is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer

(c) No transaction or account-based relationship is undertaken without following the CDD procedure.

(d) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation is specified.

(e) 'Optional'/additional information is obtained with the explicit consent of the customer after the account is opened.

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

(g) CDD Procedure is followed for all the joint account holders, while opening a joint account.

(h) Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.

(i) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.

(j) Where Permanent Account Number (PAN) is obtained, the same will be verified from the verification facility of the issuing authority. The Bank will physically verify PAN by matching it with original PAN Card and the stamp of verification will be done by concerned official of the Bank on copy of the same.

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

(l) Where Goods and Services Tax (GST) details are available, the GST number will be verified from the search/verification facility of the issuing authority.

(m) In case of an existing account where bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and / or obtain documents required as per the Risk Categorization due to non-co-operation of the customer or non-reliability of the data / information furnished to the bank, bank will close the account after following below mentioned procedure.

- **Freezing and closure of accounts**

I. In case of non-compliance of KYC requirements by the customers despite repeated reminders, bank will impose 'partial freezing' on such KYC non-compliant accounts in a phased manner.

II. During the course of such partial freezing, the account holders can revive their accounts by submitting the KYC documents as per instructions in force.

III. While imposing 'partial freezing', the bank has to ensure that the option of 'partial freezing' is exercised only after giving due notice of three months initially to the customers to comply with KYC requirements and to be followed by a reminder giving a further period of three months.

IV. Thereafter, bank may impose 'partial freezing' by allowing all credits and disallowing all debits with the freedom to close the accounts.

V. If the accounts are still KYC non-compliant after six months of imposing initial 'partial freezing', the bank would disallow all debits and credits from/to the accounts thereby, rendering them inoperative.

VI. Further, bank would have discretion to close the accounts of such customers after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions, however, need to be taken at a reasonably senior level.

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

11A. Where bank forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it will not pursue the CDD process, and instead file an STR with FIU-IND.

CHAPTER – IV

Risk Management

12. For Risk Management, Bank will adopt a risk based approach as mentioned below.

(a) Customers will be categorised as low, medium and high risk category, based on the assessment and risk perception of the Bank.

(b) Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

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

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same is specified in this policy.

Note: While preparing risk management approach FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), guidance note circulated by the RBI etc., are used as reference.

Chapter V

Customer Identification Procedure (CIP)

13. Bank will undertake identification of customers in the following cases:

(a) Commencement of an account-based relationship with the customer.

(b) Carrying out any international money transfer operations for a person who is not an account holder of the bank.

(c) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.

(d) Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.

(e) 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.

(f) When a 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.

(g) Bank will ensure that introduction is not to be sought while opening accounts.

14. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Bank may rely on customer due diligence done by a third party, subject to the following conditions:

(a) 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.

(b) Adequate steps are taken by Bank to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.

(c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.

(d) The third party shall not be based in a country or jurisdiction assessed as high risk.

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

Chapter VI

Customer Due Diligence (CDD) Procedure

Part I - Customer Due Diligence (CDD) Procedure in case of Individuals

15. For undertaking CDD, Bank will obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

(a) The Aadhaar number where,

i. He/She is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or

ii. He/She decides to submit his Aadhaar number voluntarily to a bank; or

aa) the proof of possession of Aadhaar number where offline verification can be carried out; or

ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address;

ac) the KYC Identifier with an explicit consent to download records from CKYCR; and

(b) The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and

(c) Such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the Bank:

Provided that where the customer has submitted,

i) Aadhaar number under clause (a) above to a bank, Bank will carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the Bank.

ii) Proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the Bank will carry out offline verification.

iii) An equivalent e-document of any OVD, the Bank will verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues there under and take a live photo as specified under **Annex 1**.

iv) Any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the Bank will carry out verification through digital KYC as specified under **Annex 1.**

v) KYC Identifier under clause (ac) above, Bank shall retrieve the KYC records online from the CKYCR in accordance with Section 47.

Provided that for a period not beyond such date as may be notified by the Government for a class of Bank, instead of carrying out digital KYC, the Bank pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e-document is not submitted.

Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, Bank will, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner will invariably be carried out by an official of the Bank and such exception handling will also be a part of the concurrent audit as mandated in Section 7. Bank will ensure to duly record the cases of exception handling in a centralised exception database. The database will contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database will be subjected to periodic internal audit/inspection by the Bank and will be available for supervisory review.

Explanation 1:

Bank will, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per proviso (i) above.

Explanation 2:

Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators.

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., will be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made there under.

(d) Bank shall monitor newly opened account for at least six months to observe that the activities in respect of the account are in conformity with KYC information given by the account holder. Such Risk based approach is considered necessary by bank to avoid disproportionate cost to the bank and a burdensome regime for the customers.

(e) Verification of Genuineness of Address:

i) In all instances of opening of new account, a letter of thanks will be invariably sent by the bank by speed post / approved courier at the recorded address to all the customers with dual purpose i.e.

a. Thanking them for opening the account with the bank,

b. For verification of genuineness of address furnished by the account holder to the bank.

ii) Bank will follow up closely all those cases where letter of thanks to new customers are sent to their addresses mentioned in their account opening form are returned by the postal authorities/ couriers and will ensure re-verifying their addresses.

iii) In case of existing customers, if any communication sent by bank is returned by postal authorities/ couriers, bank will ensure again to ascertain whether any change in their address has taken place.

iv) In both the above cases, Bank will ensure to re-verify their correct address by various methods/ means.

v) On being satisfied, bank will make suitable corrections in its record / system in case of change in address after following prescribed KYC procedure.

vi) Bank may even adopt such practices where address verification is done automatically like sending Pass-books, Cheque Books, Statement of Accounts etc. by Registered Post / Reliable Courier at the recorded address of customer with the bank and preserving its acknowledgements.

16. Accounts opened using OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:

i. There must be a specific consent from the customer for authentication through OTP.

ii. As a risk-mitigating measure for such accounts, Bank shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar.

iii. The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete.

iv. The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.

v. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.

vi. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 15 or as per Section 17 (V-CIP) is carried out. If Aadhaar details are used under Section 17, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.

vii. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.

viii. A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other Bank. Further, while uploading KYC information to CKYCR, Bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other Bank shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

ix. Bank shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

17. Bank may 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.

Provided that in case of CDD of a proprietorship firm, Bank shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 21 and Section 22, 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 as per Section 16.

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

Bank shall adhere to the following minimum standards to undertake V-CIP:

(a) V-CIP Infrastructure

i) The Bank will complied 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 shall be housed in own premises of the Bank and the V-CIP connection and interaction shall necessarily originate from Bank's own secured network domain. Any technology related outsourcing for the process shall be compliant with relevant RBI guidelines. Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the Bank only and all the data including video recording is transferred to the Bank's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Bank.

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 should be recorded in an auditable and alteration proof manner.

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

iv) The video recordings should 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 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 the empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

viii) The V-CIP application software and relevant APIs / web services 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 shall be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

(b) V-CIP Procedure

i) 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) Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the Bank. However, in case of call drop / disconnection, fresh session shall be 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 should 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 Section 47, using the KYC identifier provided by the customer
d. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker

Bank shall ensure to redact or blackout the Aadhaar number in terms of Section 15.

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 working 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, Bank shall ensure that the video process of the V-CIP is undertaken within three working 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, 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) 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 shall be permissible when bank take help of Banking Correspondents (BCs) facilitating the process only at the customer end. Bank shall maintain the details of the BC assisting the customer, where services of BCs are utilized. 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. 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 this policy, 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.

18. Notwithstanding anything contained in Section 15 of the Policy and as an alternative thereto, in case an individual who desires to open a bank account, the bank will open a 'Small Account' which entails the following limitations:

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:

a. The bank will obtain a self-attested photograph from the customer.

b. The designated officer of the bank certifies under his signature that the person opening the account has affixed his signature or thumb impression 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.

c. Bank will ensure 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.

d. The account will remain 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.

e. The entire relaxation provisions will be reviewed after twenty four months.

f. The account will be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, the identity of the customer will be established as per Section 15 or Section 17.

g. Foreign remittance will not be allowed to be credited into the account unless the identity of the customer is fully established as per Section 15 or Section 17.

19. KYC verification once done by one branch/office of the Bank will be valid for transfer of the account to any other branch/office of the Bank, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

Part II - CDD Measures for Sole Proprietary firms

20. For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) will be carried out.

21. In addition to the above, any two of the following documents or the equivalent e-documents there of as a proof of business/ activity in the name of the proprietary firm will also be obtained:

a) Registration certificate including Udyam Registration Certificate (URC) issued by the Government.

b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act.

c) Sales and income tax returns.

d) CST/VAT/ GST certificate

e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.

f) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.

g) 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.

h) Utility bills such as electricity, water, and landline telephone bills, etc.

22. In cases where the Bank is satisfied that it is not possible to furnish two such documents, Bank may, at its discretion, accept only one of those documents as proof of business/activity.

Provided Bank undertakes contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and will confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

Part III- CDD Measures for Legal Entities

23. For opening an account of a company, certified copies of each of the following documents or the equivalent e-documents thereof will be obtained:

a) Certificate of incorporation
b) Memorandum and Articles of Association
c) Permanent Account Number of the company
d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
e) Documents, as specified in Section 15 of this policy, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf
f) The names of the relevant persons holding senior management position and
g) The registered office and the principal place of its business, if it is different.

24. For opening an account of a partnership firm, the certified copies of each of the following documents or the equivalent e-documents thereof will be obtained:

a) Registration certificate
b) Partnership deed
c) Permanent Account Number of the partnership firm
d) Documents, as specified in Section 15 of this policy, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
e) The names of all the partners and
f) Address of the registered office, and the principal place of its business, if it is different.

25. For opening an account of a trust, certified copies of each of the following documents or the equivalent e-documents thereof will be obtained:

a) Registration certificate
b) Trust deed
c) Permanent Account Number or Form No.60 of the trust
d) Documents, as specified in Section 15 of this policy, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
e) The names of the beneficiaries, trustees, settlor and authors of the trust
f) The address of the registered office of the trust; and
g) List of trustees and documents, as specified in Section 15, for those discharging the role as trustee and authorised to transact on behalf of the trust.

26A. For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents or the equivalent e-documents thereof will be obtained:

(a) Resolution of the managing body of such association or body of individuals
(b) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals
(c) Power of attorney granted to transact on its behalf
(d) Documents, as specified in Section 15, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.
(e) Such information as may be required by the Bank to collectively establish the legal existence of such an association or body of individuals.

Explanation: Unregistered trusts/partnership firms will be included under the term 'unincorporated association'.

Explanation: Term 'body of individuals' includes societies.

26B. For opening account of a customer who is a juridical person (not specifically covered in the earlier part) such as societies, universities and local bodies like village panchayats, etc., or who purports to act on behalf of such juridical person or individual or trust, certified copies of the following documents or the equivalent e-documents thereof shall be obtained and verified:

a) Document showing name of the person authorised to act on behalf of the entity;

b) As specified in Section 15 of this policy, Documents of the person holding an attorney to transact on its behalf and

c) Such documents as may be required by the Bank to establish the legal existence of such an entity/juridical person.

Part IV -Identification of Beneficial Owner

27. For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) will be identified and all reasonable steps in terms of sub-rule (3) of Rule 9 of the Rules to verify his/her identity will be under taken keeping in view the following:

a) Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

b) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place will be obtained.

Part V - On-going Due Diligence

28. Bank will undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

29. Without prejudice to the generality of factors that call for close monitoring following types of transactions will necessarily be monitored:

a) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.

b) Transactions which exceed the thresholds prescribed for specific categories of accounts.

c) High account turnover inconsistent with the size of the balance maintained.

d) Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

For ongoing due diligence, Bank may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

30. The extent of monitoring will be aligned with the risk category of the customer.

Explanation: High risk accounts have to be subjected to more intensify monitoring.

a) A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures will be put in place.

b) It has come to the notice of RBI that accounts of Multi-level Marketing (MLM) Companies were misused for defrauding public by luring them into depositing their money with the MLM Company by promising high return. Such depositors are assured of high returns and issued post-dated cheques for interest and repayment of principal. As long as money keeps coming into the MLM Company's account from new depositors, the cheques are honored but once the chain breaks, all such post-dated instruments are dishonored. This results in fraud on the public and is a reputational risk for Banks concerned.

Bank will closely monitor the transactions in accounts of marketing firms and will carefully analyze data, in cases where a large number of cheque books are sought by the companies and there are multiple small deposits (generally in cash) across the country in one account and where a large number of cheques are issued bearing similar amounts/ dates. Bank will report such matters immediately to Reserve Bank of India (RBI) and other appropriate authorities such as FIU-IND by way of STRs on noticing unusual operations in the accounts of MLM companies.

31. Periodic Updation

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.

a) Individual Customers:

I. 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.

II. Change in address:

In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through 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, Banks, at their option, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiv), for the purpose of proof of address, declared by the customer at the time of periodic updation.

III. Accounts of customers, who were minor at the time of opening account, on their becoming major:

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

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.

IV. Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. To clarify, conditions stipulated in Section 16 are not applicable in case of updation / periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode.

Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. Bank shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

b) Customers other than individuals:

I. No change in KYC information:

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

II. Change in KYC information:

In case of change in KYC information, Bank shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

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

i) The KYC documents of the customer as per the current CDD standards are available with 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.

ii) Customer's PAN detail, if available with the Bank, is verified from the database of the issuing authority at the time of periodic updation of KYC.

iii) An Acknowledgment shall be 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.

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

v) Bank shall adopt a risk-based approach with respect to periodic updation of KYC.

vi) Bank shall ensure that Bank's KYC policy and processes on updation / periodic updation of KYC are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.

d) Bank shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business

relationship / account-based relationship and thereafter, as necessary; customers shall submit to the bank the update of such documents. This shall be done within 30 days of the update to the documents for the purpose of updating the records at Bank's end.

32. In case of existing customers, Bank will obtain the Permanent Account Number or equivalent e-document thereof or Form No.60, by such date as may be notified by the Central Government, failing which Bank will temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the Bank will give the customer an accessible notice and a reasonable opportunity to be heard. Appropriate relaxation(s) will be given for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes.
Provided further that if a customer having an existing account-based relationship with the Bank gives in writing to the Bank that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, Bank will close the account and all obligations due in relation to the account will be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

Explanation – For the purpose of this Section, "temporary ceasing of operations" in relation to an account will mean the temporary suspension of all transactions or activities in relation to that account by the Bank till such time the customer complies with the provisions of this Section. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits will be allowed.

Part VI - Enhanced and Simplified Due Diligence Procedure

A. Enhanced Due Diligence

33. Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 16): Non-face-to-face onboarding facilitates the Bank to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section includes use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. Following EDD measures shall be undertaken by Bank for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 16):

a) In case Bank has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Policy.

b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening.
c) Apart from obtaining the current address proof, Bank shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.

d) Bank shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.

e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.

f) Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

34. Accounts of Politically Exposed Persons (PEPs)

I. Bank will have the option of establishing a relationship with PEPs provided that:

a) Sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;

b) The identity of the person will have been verified before accepting the PEP as a customer;

c) The decision to open an account for a PEP is taken at a senior level in accordance with the Banks' Customer Acceptance Policy;

d) All such accounts are subjected to enhanced monitoring on an on-going basis;

e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;

f) The CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

II. These instructions will also be applicable to accounts where a PEP is the beneficial owner

B. Simplified Due Diligence

35. Simplified norms for Self Help Groups (SHGs)

a) CDD of all the members of SHG will not be required while opening the savings bank account of the SHG.

b) CDD of all the office bearers will suffice.

c) Customer Due Diligence (CDD) of all the members of SHG may be undertaken at the time of credit linking of SHGs.

36. Procedure to be followed by banks while opening accounts of foreign students

a) Banks will, at their option, open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with visa & 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.

i.) Provided that a declaration about the local address will be obtained within a period of 30 days of opening the account and the said local address is verified.

ii.) Provided further that pending the verification of address, 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 rupees fifty thousand on aggregate in the same, during the 30-day period.

b) The account will be treated as a normal NRO account, and will be operated in terms of Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of FEMA 1999.

c) Students with Pakistani nationality will require prior approval of the Reserve Bank for opening the account.

Chapter VII
Record Management

37. The following steps will be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. Bank will,

a) Maintain all necessary records of transactions between the Bank and the customer for at least five years from the date of transaction;
b) Preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;
c) Make available the identification records and transaction data to the competent authorities upon request;
d) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
e) Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

i. The nature of the transactions;
ii. The amount of the transaction and the currency in which it was denominated;
iii. The date on which the transaction was conducted; and
iv. The parties to the transaction.

f) 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;
g) Maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in hard or soft format.

Explanation. – For the purpose of this Section, the expressions "records pertaining to the identification", “identification records”, etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

37A. In case of customers who are non-profit organisations, bank will ensure that the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, Bank shall register the details on the DARPAN Portal. Bank shall also maintain such registration records for a period of five years after the business relationship between the customer and the Bank has ended or the account has been closed, whichever is later.

Chapter VIII

Reporting Requirements to Financial Intelligence Unit - India

38. Bank will furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

Suspicious Transaction Report
“Suspicious Transaction" means a transaction as defined below, including an attempted transaction, whether or not made in cash which, to a person acting in good faith;

a. Gives rise to a reasonable ground of suspicion that it may involve the proceeds of an offence specified in the schedule to the Act, regardless of the value involved; or-
b. Appears to be made in circumstances of unusual or unjustified complexity;
c. Appears to have no economic rationale or bonafide purpose; or
d. Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

It is likely that in some cases transactions are abandoned / aborted by customers on being asked to give some details or to provide documents. Branches will report all such attempted transactions in STRs even if not completed by customers, irrespective of the amount of the transaction.

39. The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist Bank in the preparation of prescribed reports will be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website will be used by the Bank till suitable technological tools for extracting CTR/STR from live transaction data are not installed/adopted.

40. While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule will be constituted as a separate violation. Bank will not put any restriction on operations in the accounts where an STR has been filed. Bank will keep the fact of furnishing of STR strictly confidential. It will be ensured that there is no tipping off to the customer at any level. **(Tentative list of STR is attached as per Annex – 4)**

41. Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers will be put in to use as a part of effective identification and reporting of suspicious transactions.

Chapter IX
Requirements/obligations under International Agreements Communications from International Agencies –

42. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:

(a) In terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, they do not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). The details of the two lists are as under**:**

i. The **"ISIL (Da'esh) &Al-Qaida Sanctions List**", established and maintained pursuant to Security Council resolutions 1267/1989/2253, which includes names of individuals and entities associated with the Al-Qaida is available at https://scsanctions.un.org/ohz5jen-al-qaida.html

ii. The **"Taliban Sanctions List"**, established and maintained pursuant to Security Council resolution 1988 (2011)**,** which includes names of individuals and entities associated with the Taliban is available at https://scsanctions.un.org/3ppp1en-taliban.htm

Bank will also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, will be verified by Bank on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Bank for meticulous compliance.

(b) Details of accounts resembling any of the individuals/entities in the lists will be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated February 02, 2021.

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

(d) Freezing of Assets under Section 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated February 2, 2021 (Annex II of RBI KYC Master Direction-2016) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA.

43. Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

(a) Bank will ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January30, 2023, by the Ministry of Finance, Government of India (As per attachment as Annex-III in RBI's KYC Master Direction updated as on May 04, 2023).

(b) In accordance with paragraph 3 of the aforementioned Order, Bank will ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

(c) Further, Bank should run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

(d) In case of match in the above cases, Bank need to immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO- Director, FIU-India has been designated as the CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. Bank need to file an STR with FIUIND covering all transactions in the accounts, covered above, carried through or attempted.

(e) Bank may refer to the designated list, as amended from time to time, available on the portal of FIU-India.

(f) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, Bank must prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.

(g) In case an order to freeze assets under Section 12A is received by the Bank from the CNO, Bank must, without delay, take necessary action to comply with the Order.

(h) The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing should be forwarded by Bank along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

44. Bank should regularly verify, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at https://www.mea.gov.in/Implementationof- UNSC-Sanctions-DPRK.htm, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government.

44A. In addition to the above, Bank should take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act.

45. Jurisdictions that do not or insufficiently apply the FATF Recommendations

(a) FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, will be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement will be taken into account.
(b) Special attention will be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

Explanation: The process referred to in (a) & (b) do not preclude Bank from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.
(c) The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations will be examined, and written findings together with all documents will be retained and will be made available to Reserve Bank/other relevant authorities, on request.

Chapter X

Other Instructions

46. Secrecy Obligations and Sharing of Information:

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

(b) 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.

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

(d) The exceptions to the said rule will be as under:

i. Where disclosure is under compulsion of law
ii. Where there is a duty to the public to disclose,
iii. The interest of Bank requires disclosure and
iv. Where the disclosure is made with the express or implied consent of the customer.

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

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

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

c) Bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' **(Annexure – A)** and 'Legal Entities' **(Annexure A1 & Annexure A2)** as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.

d) The 'live run' of the CKYCR has started with effect from July 15, 2016 in phased manner beginning with new 'individual accounts'. Accordingly, Bank shall take the following steps:

(i) Bank has to invariably upload the KYC data pertaining to all new individual accounts opened on or after January 1, 2017 with **CKYCR** in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

e) Bank has to upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules ibid. The KYC records have to be uploaded as per the LE Template released by CERSAI.

f) Once KYC Identifier is generated by CKYCR, Bank shall ensure that the same is communicated to the individual/LE as the case may be.

g) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, Bank shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above mentioned dates as per point No. d (i) and (e) respectively at the time of periodic updation as specified in Section 31 of this Policy, or earlier, when the updated KYC information is obtained / received from the customer.

h) Bank has to ensure that during periodic updation, the customers are migrated to the current CDD standard.

i) 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 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.

48. Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

Under FATCA and CRS, Bank will adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, will take following steps for complying with the reporting requirements:
(a) Register on the related e-filling portal of Income Tax Department as Reporting Financial Institutions at the link https://incometaxindiaefiling.gov.in/ post login --> My Account --> Register as Reporting Financial Institution,

(b) Submit online reports by using the digital signature of the 'Designated Director' by either uploading the Form 61B or 'NIL' report, for which, the schema prepared by Central Board of Direct Taxes (CBDT) will be referred to.

Explanation: Bank will refer to the spot reference rates published by Foreign Exchange Dealers' Association of India (FEDAI) on their website at http://www.fedai.org.in/RevaluationRates.aspx for carrying out the due diligence procedure for the purposes of identifying reportable accounts in terms of Rule 114H.

(c) Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.

(d) Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.

(e) Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.

(f) Ensure compliance with updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site http://www.incometaxindia.gov.in/Pages/default.aspx. Bank may take note of the following:
i. updated Guidance Note on FATCA and CRS
ii. A press release on 'Closure of Financial Accounts' under Rule 114H (8).

49. Period for presenting payment instruments

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

50. Operation of Bank Accounts & Money Mules

The instructions on opening of accounts and monitoring of transactions will be strictly adhered to, in order to minimise the operations of "Money Mules" which are 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 which act as "money mules." Bank is aware that if it is established that an account opened and operated is that of a Money Mule, it will be deemed that the bank has not complied with these directions.

51. Collection of Account Payee Cheques:

Account payee cheques for any person other than the payee constituent will not be collected. Bank will, at own option, collect account payee cheques drawn for an amount not exceeding rupees fifty thousand to the account of own customers who are co-operative credit societies, provided the payees of such cheques are the constituents of such co-operative credit societies.

52. (a) A Unique Customer Identification Code (UCIC) will be allotted while entering into new relationships with individual customers as also the existing customers by banks
(b) The bank will, at own option, not issue UCIC to all walk-in/occasional customers such as buyers of pre-paid instruments/purchasers of third party products provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

53. Introduction of New Technologies – Credit Cards/Debit Cards/ Smart Cards/Gift Cards/Mobile Wallet/ Net Banking/ Mobile Banking/RTGS/ NEFT/ECS/IMPS etc.

Adequate attention will be paid by Bank to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it will be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing new products/services/technologies. Representatives of third party corporate agencies for marketing of various products will be subjected to the due diligence and KYC measures.

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

Further, Bank shall ensure:

(a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
(b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

54. Wire transfer

A. Information requirements for wire transfers for the purpose of KYC guidelines:

i. In Domestic wire transfer, where the originator is an account holder of the ordering Bank, shall be accompanied by accurate, complete, and meaningful originator and beneficiary information as mentioned below:

a. name of the originator;
b. the originator account number where such an account is used to process the transaction;
c. the originator's address, or national identity number, or customer identification number, or date and place of birth;
d. name of the beneficiary; and
e. the beneficiary account number where such an account is used to process the transaction.

In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

ii. In case of batch transfer, where several individual domestic wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they (i.e., individual transfers) are exempted from the requirements of clause (i) above in respect of originator information, provided that they include the originator's account number or unique transaction reference number, as mentioned above, and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

iii. Domestic wire transfers of rupees fifty thousand and above, where the originator is not an account holder of the ordering Bank, shall also be accompanied by originator and beneficiary information as indicated.

iv. Bank shall ensure that all the information on the wire transfers shall be immediately made available to appropriate law enforcement and/or prosecutorial authorities as well as FIU-IND on receiving such requests with appropriate legal provisions.

vi. The wire transfer instructions are not intended to cover the following types of payments:

a. Any transfer that flows from a transaction carried out using a credit card / debit, including through a token or any other similar reference string associated with the card, for the purchase of goods or services, so long as the credit or debit card number or reference number accompanies all transfers flowing from the transaction. However, when a credit or debit card is used as a payment system to effect a person-to-person wire transfer, the wire transfer instructions shall apply to such transactions and the necessary information should be included in the message.
b. Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are regulated financial institutions acting on their own behalf.

B. Responsibilities of ordering Bank and beneficiary Bank, effecting wire transfer, are as under:

i. Ordering Bank:

a. The ordering Bank shall ensure that all qualifying domestic wire transfers {viz., transactions as per clauses (iii) and (iv) of paragraph 'A' above}, contain required and accurate originator information and required beneficiary information, as indicated above.
b. Customer Identification shall be made if a customer, who is not an account holder of the ordering Bank, is intentionally structuring domestic wire transfers below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish identity and if the same transaction is found to be suspicious, STR may be filed with FIU-IND in accordance with the PML Rules.
c. Ordering Bank shall not execute the wire transfer if it is not able to comply with the requirements stipulated.

ii. Beneficiary Bank:

a. Beneficiary Bank should take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers and qualifying domestic wire transfers {viz., transactions as per clauses (iii) and (iv) of paragraph 'A' above}, that lack required originator information or required beneficiary information.
b. Beneficiary Bank should have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

C. Other Obligations

i. Obligations in respect of Bank's engagement or involvement with unregulated entities in the process of wire transfer

Bank should be cognizant of their obligations under these instructions and ensure strict compliance, in respect of engagement or involvement of any unregulated entities in the process of wire transfer. More specifically, whenever there is involvement of any unregulated entities in the process of wire transfers, the concerned Bank shall be fully responsible for information, reporting and other requirements and therefore shall ensure, inter alia, that,

i. there is unhindered flow of complete wire transfer information, as mandated under these directions, from and through the unregulated entities involved;

ii. the agreement / arrangement, if any, with such unregulated entities by Bank clearly stipulates the obligations under wire transfer instructions; and

iii. a termination clause is available in their agreement / arrangement, if any, with such entities so that in case the unregulated entities are unable to support the wire information requirements, the agreement / arrangement can be terminated. Existing agreements / arrangements, if any, with such entities shall be reviewed within three months to ensure aforementioned requirements.

ii. Bank responsibility to fulfil record management requirements

Complete originator and beneficiary information relating to wire transfers shall be preserved by the Bank involved in the wire transfer, in accordance with Section 37 of this policy.

55. Issue and Payment of Demand Drafts, etc.

Any remittance of funds by way of demand draft, mail/telegraphic transfer/NEFT/IMPS or any other mode and issue of travellers' cheques for value of rupees fifty thousand and above will be effected by debit to the customer's account or against cheques and not against cash payment.
Further, the name of the purchaser will be incorporated on the face of the demand draft, pay order, banker's cheque, etc., by the issuing bank for such instruments.

56. Quoting of PAN

Permanent account number (PAN) or equivalent e-document thereof of customers will be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to bank, as amended from time to time. Form 60 will be obtained from persons who do not have PAN or equivalent e-document thereof.

57. Selling Third party products

Bank acting as agents while selling third party products as per regulations in force from time to time will comply with the following aspects for the purpose of this policy:

(a) The identity and address of the walk-in customer will be verified for transactions above rupees fifty thousand as required under point No. 13 (e) of this policy.

(b) Transaction details of sale of third party products and related records will be maintained as prescribed in Chapter VII Section 37.

(c) AML software capable of capturing, generating and analysing 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) Transactions involving rupees fifty thousand and above will be undertaken only by:
• Debit to customers' account or against cheques; and
• obtaining and verifying of the PAN given by the account-based as well as walk-in customers.
(e) Instruction at 'd' above will also apply to sale of Banks' own products for rupees fifty thousand and above.

58. Hiring of Employees and Employee training

a) Adequate screening mechanism as an integral part of their personnel recruitment/hiring process will be put in place.

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

c) On-going employee training programme will be put in place so that the members of staff are adequately trained in AML/CFT policy. The focus of the training will be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff will 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.

59. Review of Policy

The KYC Policy is subject to modifications as and when necessary with the approval of the Board. Audit & inspection will submit the policy to the board for Review at annual intervals.

Annexure 1

Digital KYC Process

A. The Bank will develop an application for digital KYC process which will be made available at customer touch points for undertaking KYC of their customers and the KYC process will be undertaken only through this authenticated application of the Bank.

B. The access of the Application will be controlled by the Bank and it should be ensured that the same is not used by unauthorized persons. The Application will be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by Bank to its authorized officials.

C. The customer, for the purpose of KYC, will visit the location of the authorized official of the Bank or vice-versa. The original OVD will be in possession of the customer.

D. The Bank will ensure that the live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the Bank will put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by Bank) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

E. The Application of the Bank will have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person will come into the frame while capturing the live photograph of the customer.

F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), will be captured vertically from above and water-marking in readable form as mentioned above will be done. No skew or tilt in the mobile device will be there while capturing the live photograph of the original documents.

G. The live photograph of the customer and his original documents will be captured in proper light so that they are clearly readable and identifiable.

H. Thereafter, all the entries in the CAF will be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

I. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' will be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the Bank will not be used for customer signature. The Bank must check that the mobile number used in customer signature will not be the mobile number of the authorized officer.

J. The authorized officer will provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official will be verified with One Time Password (OTP) which will be sent to his mobile number registered with the Bank. Upon successful OTP validation, it will be treated as authorized officer's signature on the declaration. The live photograph of the authorized official will also be captured in this authorized officer's declaration.

K. Subsequent to all these activities, the Application will give information about the completion of the process and submission of activation request to activation officer of the Bank, and also generate the transaction-id/reference-id number of the process. The authorized officer will intimate the details regarding transaction-id/reference-id number to customer for future reference.

L. The authorized officer of the Bank will check and verify that:-

(i) Information available in the picture of document is matching with the information entered by authorized officer in CAF.

(ii) Live photograph of the customer matches with the photo available in the document. and

(iii) All of the necessary details in CAF including mandatory field are filled properly.

M. On Successful verification, the CAF will be digitally signed by authorized officer of the Bank who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

Bank may use the services of Business Correspondent (BC) for this process.

Annexure – 2

Risk Categorization of Customers based on below mentioned parameters:

- **Non-Financial Parameter**

Parameter	High Risk	Medium Risk	Low Risk
Type of Customer	i) Private Ltd. Company ii) Public Ltd Co. (Closely held) iii) Trusts iv) Charities v) Politically Exposed Persons vi) Customers having adverse publicity. vii) NRIs of Indian Origin. viii) Firms with operative transactions authorized by sleeping partner	i) Public Ltd companies (widely held)	i) Salaried persons. ii) Pensioners iii) Professional & Self-employed persons iv) Agriculturist v) Self Help Groups vi) Government companies vii) Public Sector companies viii) Government Departments
Business Activity	i) Jewellery ii) Chit Funds iii) Finance Companies iv) Foreign Exchange, v) Money Market Brokers vi) Travel Agencies vii) Export / Import Trade	i) Commodity Trade ii) Hotel Business	i) Industry ii) Plantations iii) Retail Trade iv) Agriculture and other Allied Activities v) Service Class vi) Other people belonging to low strata group
Source (Nationality) of funds / Location of Customer	Foreign Remittances from national of Gulf, Pakistan, Afghanistan, Libya and Syria, Developing Countries, African Countries, South American Countries	Foreign Remittance from national of Eastern Block Countries, Indonesia, Burma, Malaysia, Singapore and Thailand, Russia and China	Foreign Remittance from nationals of United States and European Countries. Foreign Remittances from NRIs & persons of Indian origin.
Composition of partners, directors	Entirely Foreign nationality, Firms with sleeping partners.	A mix of Indian and Foreign nationals	Exclusively Indian nationals

- **Financial Parameter**

Parameter	High Risk	Medium Risk	Low Risk
Balance Outstanding (All deposit accounts) (SB+ CA + TD).	NRIs/Customer having aggregate deposit Rs.50 lakhs & above Non-Face to face customers with aggregate deposit of Rs.10 lakhs and above.	NRIs/Customer having aggregate deposit Rs.25 lakhs and above, but less than Rs.50 lakhs.	NRIs/Customer having aggregate deposit less than Rs.25 lakhs.
Turnover Basis (Cumulative in F.Y.) (All Deposit Account i.e. SB + CA + TD).	Above Rs. 50 lakhs (for other than SME customers) Above Rs.25 Crores (for SME customers).	Above Rs. 10 lacs but up to Rs.50 lakhs (for other than SME customers) Above Rs.10 Crores but less than Rs.25 Crores (for SME customers).	Up to Rs.10 lacs (for other than SME customers) Up to Rs.10 Crores (for SME customers).
Cash Transaction Basis (Cumulative in F.Y.) (All deposit accounts i.e. SB + CA + TD).	All the accounts reported in CTR having credit or debit summation above Rs.50 lacs.	All the accounts reported in CTR having credit or debit summation above Rs.10 lacs but up to Rs.50 lacs.	All the accounts which are having credit or debit summation up to Rs.10 lacs.

Annexure– 3

Indicative List of High / Medium risk customers:

The following lists are indicative and can be expanded. The bank has the option to upgrade the risk categorization (i.e. medium to high) for any specific industry / segment.

Characteristics of High Risk Customers

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
19. Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution.
20. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc.
21. 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)
22. Money Service Business including seller of Money Transmission / Check Cashing / Currency Dealing or Exchange

23. Business accepting third party cheques (except supermarkets or retail stores that accept payroll cheques /cash payroll cheques) 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.

Characteristics of Medium Risk Customers:

1. Non-Bank Financial Institution
2. Stock brokerage
3. Import / Export
4. Gas Station
5. Car / Boat / Plane Dealership
6. Electronics (wholesale)
7. Travel agency
8. Used car sales
9. Telemarketers
10. Providers of telecommunications service, internet café, IDD call service, phone cards, phone center
11. Dot-com company or internet business
12. Pawnshops
13. Auctioneers
14. Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.
15. Sole Practitioners or Law Firms (small, little known)
16. Notaries (small, little known)
17. Secretarial Firms (small, little known)
18. Accountants (small, little known firms)
19. Venture capital companies

Annexure – 4

Indicative list of Behaviour Based Alert Indicators for Branches/ Departments- Part- I

S. No.	Alert Indicator	Indicative Suspicion
1.	Customer left without opening account	Customer did not open account after being informed about KYC requirements
2.	Customer offered false or forged identification documents	Customer gives false identification documents or documents that appears to be counterfeited, altered or inaccurate
3.	Identity documents are not verifiable	Identity documents presented are not verifiable i.e. Foreign documents etc.
4.	Address found to be non- existent	Address provided by the customer is found to be non-existent
5.	Address found to be wrong	Customer not staying at address provided during account opening
6.	Difficult to identify beneficial owner	Customer uses complex legal structures or where it is difficult to identify the beneficial owner
7.	Customer is being investigated for criminal Offences	Customer has been the subject of inquiry from any law enforcement agency relating to criminal offences
8.	Customer is being investigated for TF offences	Customer has been the subject of inquiry from any law enforcement agency relating to TF or terrorist activities
9.	Adverse media report about criminal activities of Customer	Match of customer details with persons reported in local media / open source for criminal offences
10.	Adverse media report about TF or terrorist activities of customer	Match of customer details with persons reported in local media / open source for terrorism or terrorist financing related activities
11.	Customer did not complete Transaction	Customer did not complete transaction after queries such source of funds etc.
12.	Customer is nervous	Customer is hurried or nervous
13.	Customer is over cautious	Customer over cautious in explaining genuineness of the transaction.
14.	Customer provides inconsistent information	Customer changes the information provided after more detailed information is requested. Customer provides information that seems minimal, possibly false or inconsistent.
15.	Customer acting on behalf of a third party	Customer has vague knowledge about amount of money involved in the transaction. Customer taking instructions for conducting transactions. Customer is accompanied by unrelated Individuals.
16.	Multiple customers working as a group	Multiple customers arrive together but pretend to ignore each other
17.	Customer avoiding nearer branches	Customer travels unexplained distances to conduct transactions

18.	Customer offers different identifications on different occasions	Customer offers different identifications on different occasions in an apparent attempt to avoid linkage of multiple transactions
19.	Customer wants to avoid reporting	Customer makes inquiries or tries to convince staff to avoid reporting
20.	Customer could not explain source of funds	Customer could not explain source of funds
21.	Transaction is unnecessarily complex	Transaction is unnecessarily complex for its stated purpose
22.	Transaction has no economic rationale	The amounts or frequency or the stated reason of the transaction does not make sense for the particular customer
23.	Transaction inconsistent with business	Transaction involving movement of which is inconsistent with the customer's business
24.	Unapproved inward remittance in NPO	Foreign remittance received by NPO not approved by FCRA
25.	Complaint received from Public	Complaint received from public for abuse of account for committing fraud etc.
26.	Alert raised by agent	Alert raised by agent for suspicion
27.	Alert raised by other institution	Alert raised by other institutions, subsidiaries or business associates including cross border referral

Table showing Details deleted from RBI KYC Master Direction 2016 issued by RBI (vide Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016 (updated upto 04.05.2023) which are not included in KYC policy of Bank as per comments made in Remarks column against each point.

Section No.	Details	Remarks
3 Definitions (b)	(b) Terms bearing meaning assigned in this Directions, unless the context otherwise requires, shall bear the meanings assigned to them below: ii. **17Correspondent Banking:** Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Respondent banks may be provided with a wide range of services, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable through accounts and foreign exchange services. xii. 19Payable-through accounts: The term payable-through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf. **xiv. "Regulated Entities" (REs) means** a. all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licensed under Section 22 of Banking Regulation Act, 1949, which as a group will be referred as 'banks' b. All India Financial Institutions (AIFIs) c. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs). d. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers) e. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator. **xv.** "Shell bank" means a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group. **xvii. 22"Wire transfer" related definitions:** e. **Cross-border wire transfer:** Cross-border wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.	Not used in Policy
Chapter –II Point no-4	4. (a) There shall be a Know Your Customer (KYC) policy duly approved by the Board of Directors of REs or any committee of the Board to which power has been delegated. [24](b) REs shall ensure that a group-wide policy is implemented for the purpose of discharging obligations under the provisions of Chapter IV of the Prevention of Money-laundering Act, 2002 (15 of 2003). [25](c) REs' policy framework should seek to ensure compliance with PML Act/Rules, including regulatory instructions in this regard and	Guideline for implementing KYC Policy in Bank

	should provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, REs may also consider adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.	
23	(c) 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 the account.	Our all branches are under CBS
24	24. Simplified procedure for opening accounts by Non-Banking Finance Companies (NBFCs): In case a person who desires to open an account is not able to produce documents, as specified in Section 16, NBFCs may at their discretion open accounts subject to the following conditions: (a) The NBFC will obtain a self-attested photograph from the customer. (b) The designated officer of the NBFC certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence. (c) The account will remain operational initially for a period of twelve months, within which CDD as per Section 16 will be carried out. (d) Balances in all their accounts taken together will not exceed rupees fifty thousand at any point of time. (e) The total credit in all the accounts taken together will not exceed rupees one lakh in a year. (f) The customer will be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (d) and (e) above are breached by him. (g) The customer will be notified when the balance reaches rupees forty thousand or the total credit in a year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account will be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in direction (d) and (e) above.	Point related to NBFC
42	42. Client accounts opened by professional intermediaries**:** Bank will ensure while opening client accounts through professional intermediaries, that: (a) Clients will be identified when client account is opened by a professional intermediary on behalf of a single client. (b) Bank will have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. (c) Bank 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. (d) All the beneficial owners will be identified where funds held by the intermediaries are not co-mingled at the level of BANK, and there are 'sub-accounts', each of them attributable to a beneficial owner, or where	Such facility does not exist in bank and such account are not opened in Bank

	such funds are co-mingled at the level of BANK, the BANK will look for the beneficial owners. (e) Bank will, at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers. (f) The ultimate responsibility for knowing the customer lies with the BANK.	
45	**45. Simplified KYC norms for Foreign Portfolio Investors (FPIs)** Accounts of FPIs which are eligible/ registered as per SEBI guidelines, for the purpose of investment under Portfolio Investment Scheme (PIS), will be opened by accepting KYC documents as detailed in Annex III, subject to Income Tax (FATCA/CRS) Rules. Provided that banks will obtain undertaking from FPIs or the Global Custodian acting on behalf of the FPI that as and when required, the exempted documents as detailed in Annex III will be submitted.	Such facility not exist
47 Explanation	Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND will have powers to issue guidelines to the Bank for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.	FIU-power not required in policy
48 Para	The Principal Officers of those Bank, whose all branches are not fully computerized, will have suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in	Our all branches are computerised hence not applicable
63	**63. Correspondent Banks** Banks will have a policy approved by their Boards, or by a committee headed by the Chairman/CEO/MD to lay down parameters for approving correspondent banking relationships subject to the following conditions: (a) Sufficient information in relation to the nature of 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 will be gathered. (b) Post facto approval of the Board at its next meeting will be obtained for the proposals approved by the Committee. (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, the correspondent bank will be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking on-going 'due diligence' on them. (e) The correspondent bank will ensure that the respondent bank is able to provide the relevant customer identification data immediately on	No such facility / arrangement with Bank

	request. (f) Correspondent relationship will not be entered into with a shell bank. (g) It will be ensured that the correspondent banks do not permit their accounts to be used by shell banks. (h) Banks will be cautious with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations. (i) Banks will ensure that respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.	
64 (A) 64(B)	(a) All cross-border wire transfers including transactions using credit or debit card will be accompanied by accurate and meaningful originator information such as name, address and account number or a unique reference number, as prevalent in the country concerned in the absence of account. Exception: Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions will be exempt from the above requirements. **ii. Intermediary Bank:** a. Bank processing an intermediary element of a chain of wire transfers shall ensure that all originator and beneficiary information accompanying a wire transfer is retained with the transfer. b. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary Bank shall keep a record, for at least five years, of all the information received from the ordering financial institution or another intermediary Bank. c. Intermediary Bank shall take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing. d. Intermediary Bank shall have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules. **iv. Money Transfer Service Scheme (MTSS)** providers are required to comply with all of the relevant requirements of this Section, whether they are providing services directly or through their agents. In the case of a MTSS provider that controls both the ordering and the beneficiary side of a wire transfer, the MTSS provider: a. shall take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and b. shall file an STR with FIU, in accordance with the PML Rules, if a transaction is found to be suspicious. 64(C).Other Obligations **ii. Bank's responsibility while undertaking cross-border wire transfer with respect to name screening (such that they do not process cross-border transactions of designated persons and entities)** REs are prohibited from conducting transactions with designated	No cross border direct transaction done by bank

	persons and entities and accordingly, in addition to compliance with Chapter IX of the Master Direction, REs shall ensure that they do not process cross-border transactions of designated persons and entities.	
67 (e)	**(e) Instruction for (**transactions involving rupees fifty thousand and above shall be undertaken only by: • debit to customers' account or against cheques; and • obtaining and verifying the PAN given by the account-based as well as **walk-in customers.)** shall also apply to sale of REs' own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.	No such product available with bank
68	68. At-par cheque facility availed by co-operative banks (a) The 'at par' cheque facility offered by commercial banks to co-operative banks will be monitored and such arrangements be reviewed to assess the risks including credit risk and reputational risk arising therefrom. (b) The right to verify the records maintained by the customer cooperative banks/ societies for compliance with the extant instructions on KYC and AML under such arrangements will be retained by banks. (c) Cooperative Banks will: i. ensure that the 'at par' cheque facility is utilised only: a. for their own use, b. for their account-holders who are KYC complaint, provided that all transactions of rupees fifty thousand or more are strictly by debit to the customers' accounts, c. for walk-in customers against cash for less than rupees fifty thousand per individual. ii. 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 honouring such instruments. iii. ensure that 'At par' cheques issued are crossed 'account payee' irrespective of the amount involved.	No such facility provided by Bank or not having any arrangement with co-op Banks
69	69. Issuance of Prepaid Payment Instruments (PPIs): PPI issuers will ensure that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India through their Master Direction are strictly adhered to.	No product
71	71. Adherence to Know Your Customer (KYC) guidelines by NBFCs/RNBCs and persons authorised by NBFCs/RNBCs including brokers/agents etc. (a) Persons authorised by NBFCs/ RNBCs for collecting the deposits and their brokers/agents or the like, will be fully compliant with the KYC guidelines applicable to NBFCs/RNBCs. (b) All information will be made available to the Reserve Bank of India to verify the compliance with the KYC guidelines and accept full consequences of any violation by the persons authorised by NBFCs/RNBCs including brokers/agents etc. who are operating on their behalf.	Applicable to NBFC/ RNBC

	(c) The books of accounts of persons authorised by NBFCs/RNBCs including brokers/agents or the like, so far as they relate to brokerage functions of the company, will be made available for audit and inspection whenever required.	
72	72. With the issue of these directions, the instructions / guidelines contained in the circulars mentioned in the Appendix, issued by the Reserve Bank stand repealed.	Repeal provisions of master direction not applicable to policy
73	73. All approvals / acknowledgements given under the above circulars will be deemed as given under these directions.	
74	74. All the repealed circulars are deemed to have been in force prior to the coming into effect of these directions	