Final –

KYC/AML POLICY
2023-24

CONFIDENTIAL (For Internal Use Only)

PASSED AT THE BOARD OF DIRECTORS MEETING
HELD ON 29-04-23

CHIEF EXECUTIVE OFFICER CHAIRMAN

RISK & COMPLIANCE DEPT.
CITIZENCREDIT CO-OP. BANK LTD

CITIZENCREDIT CO-OP. BANK LTD. C.A.O. Malad

Table of Contents

Policy Guidelines on KYC/AML/CFT 2022-23

1. INTRODUCTION

1.1 Bank has in place a policy on KNOW YOUR CUSTOMER (KYC) norms and ANTI MONEY LAUNDERING (AML) measures approved by the Board in its meeting. The policy was based on then guidelines issued by Reserve Bank of India (RBI).

1.2 The KYC guidelines have regularly been revisited by RBI in the context of the recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT) and has advised banks to follow certain customer identification procedures for opening of accounts and monitoring transactions of suspicious nature for the purpose of reporting it to the appropriate authority.

1.3 The Bank has advised banks to put in place a policy on KYC and AML measures including the recommendations with the approval of the Board and shall take steps to implement the provisions of the aforementioned Act and Rules, including operational instructions issued in pursuance of such amendment(s).

1.4 The Bank to follow the guidelines under Section 35A of the Banking Regulation Act, 1949 and Rule 7 of Prevention of Money-Laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 along with amendments to the Prevention of Money Laundering (PML) Act, 2002. The Bank to note any contravention thereof or non-compliance may attract penalties under Banking Regulation Act.

2. OBJECTIVES OF THE POLICY

2.1 To lay down policy framework for abiding by the KYC norms and AML measures as set out by RBI, based on the recommendations of the FATF and the paper issued on Customer Due Diligence (CDD) for banks issued by the Basel Committee on Banking Supervision.

2.2 To prevent the Bank from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.

2.3 To enable the Bank to know / understand its customers and their financial dealings better, which in turn would help it to manage its risks prudently.

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

2.5 To take necessary steps to ensure that the relevant staff are adequately trained in KYC/AML procedures.

2.6 The Board approved policy on KYC/AML/CFT is subject to annual review.

3. OVERVIEW

This policy document on KYC norms / AML standards / Combating of Financing of Terrorism (CFT) / Obligation of banks under Prevention of Money Laundering Act, 2002 as applicable to our Bank, for conducting AD Category-II transactions and Depository Services, sets the standards for implementation of KYC for the proper management of risks associated with money laundering and terrorist financing with the objective to prevent misuse of funds and Bank's reputation by criminal elements for money laundering or terrorist financing activities.

The Policy is framed with the following purpose –

- Create an awareness & guidance on the legal and regulatory frame work for AML/CFT requirements and systems across the Bank among customers, management & employees.
- Interpret, implement & comply with the obligations under the PMLA and other relevant

regulations.

- Help the Bank to align its operations with good international industry practice in AML/CFT procedures through a proportionate risk based approach.
- Provide a framework for the Bank to design and implement the systems and controls necessary to mitigate the risks of the bank being used in connection with money laundering and terrorist financing.
- Identify customers who might use the Bank for illegal activities.

The document also enables the Bank to know/understand its customers and their financial dealings, in turn to help manage risk prudently.

The document details out the four key elements on KYC being
a. Customer Acceptance Policy;
b. Customer Identification Procedures;
c. Monitoring of Transactions; and
d. Risk Management.

The document also highlights the role of the Bank in reporting to the Financial Intelligence Unit (FIU)-India. It is expected that this document will assist branches in complying with KYC/AML/CFT guidelines while simultaneously meeting the Bank's objective of providing banking services to customers. Detailed operational instructions on KYC/ AML/ CFT will be issued from time to time.

4. DEFINITIONS

4.1 **Aadhaar number,** as defined in the Aadhaar and Other Law (Amendment) Ordinance, 2019, means an identification number issued to an individual under sub-section (3) of section 3 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), and includes any alternative virtual identity generated under sub-section (4) of that section.

4.2 **Authentication**, in the context of Aadhaar authentication, means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository (CIDR) for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it, as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

4.3 **Beneficial Owner:** Rule 9(1A) of the Prevention of Money Laundering Rules, 2005 requires that every banking company, and financial institution, as the case may be, shall identify the beneficial owner and take all reasonable steps to verify his identity. The term "beneficial owner" has been defined as the natural person who ultimately owns or controls a client and / or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person.
A juridical person is an Entity that is not a single natural person (as a human being), authorized by law with duties and rights, recognized as a legal authority having a distinct identity, a legal personality (Also known as artificial person, juridical entity, juristic person, or legal person).

Procedure for determination of Beneficial Ownership is as under:

a) Where the client is a **company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.
Explanation- For the purpose of this sub-clause-
1. "Controlling ownership interest" means ownership of or entitlement to more than twenty-five percent (**25%**) of shares or capital or profits of the company;
2. "Control" shall 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 client is a **partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of/entitlement to more than fifteen percent (**15%**) of capital or profits of the partnership;
c) where the client is an **unincorporated association** or **body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property (**15%**) or capital or profits of such 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 client is a **trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent (**15%**) or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and
e) where the client or the owner of the controlling interest is a **company listed on a stock exchange**, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.
Beneficial owner declaration to be obtained while opening accounts and also during re-kyc/ periodic kyc of Non-Individuals.

4.4 **Customer** means a person who is engaged in a financial transaction or activity and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
The expression 'Customer' in the simple sense means, one who transacts himself with the bank subject to certain terms and conditions as imposed by the Banker. In other words, a person, who maintains an account with the bank, may be regarded as customer.
The term 'customer of a bank' has not been defined in the Banking Regulation Act, 1949 or any other Act. By the term it is generally understood or means an account holder of bank. But this general understanding of the term has been qualified by banking experts and judgements of law courts. Hence, there is no satisfactory definition for the term 'customer'. However, some attempts were made to define the term 'customer' as stated below:
As per RBI circular dated 01.07.2008, for the purpose of KYC Policy a **'customer'** includes:
- a person or entity that maintains an **account and /or has a business relationship** with the bank.
- one on whose behalf the account is maintained **(i.e. the beneficial owner)**
- beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
- any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

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

Customer Due Diligence measures to be taken for:

i) New customers: while commencing an account-based relationship.

ii) Existing clients: at an interval of two/eight/ten years in respect of high/medium/low risk clients respectively.

iii) Ongoing due diligence of existing clients in order to ensure that their transactions are consistent with the bank's knowledge of the client, his business and risk profile and where necessary, the source of funds.

4.6 Customer identification means undertaking the process of CDD.

4.7 Certified Copy - Obtaining a certified copy shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorized officer of the bank.

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:

i. Notary Public abroad,

ii. Court Magistrate,

iii. Judge,

iv. Indian Embassy/Consulate General in the country where the non-resident customer resides.

4.8 Central KYC Records Registry (CKYCR) means an entity defined under Rule 2(1) (aa) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

Government of India has authorised the Central Registry of Securitization 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.

The 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' and 'Legal Entities' as the case may be.

4.9 Designated Director refers to the Managing Director, duly authorized by the BOD to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules. The Designated Director shall oversee the compliance position of AML norms in the Bank.

4.10 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 authorized officer of the Bank.

4.11 Digital Signature shall 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).

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document that has been sent is unchanged.

4.12 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.

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

4.14 Non-profit organisations (NPO) means any entity or organization that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.
All transactions involving receipts by NPOs of value more than Rs.10 lakhs, or its equivalent in foreign currency will be reported by Head Office to FIU-IND. However, if the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.10 lakhs, the Bank shall consider filing a Suspicious Transaction Report to FIU-IND.

4.15 Officially Valid Document (OVD) are:

1. Passport,
2. Driving licence,
3. Proof of possession of Aadhaar number *
4. Voter's Identity Card issued by the Election Commission of India,
5. Job card issued by NREGA duly signed by an officer of the State Government and
6. Letter issued by the National Population Register containing details of name and address.

Provided that
A)* Where the client submits his **proof of possession of Aadhaar number** as an officially valid document (OVD), he may submit it in such form as are issued by the Unique Identification Authority of India (UIDAI) and Proof of possession of Aadhaar shall include the following:
(a) Aadhaar letter issued by UIDAI which carries name, address, gender, photo and date of birth details of the Aadhaar number holder.
(b) Downloaded Aadhaar (e-Aadhaar) which carries name, address, gender, photo and date of birth details of the Aadhaar number holder in similar form as in printed Aadhaar letter. This is digitally signed by UIDAI.
(c) Aadhaar Secure QR code generated and digitally signed by UIDAI containing carries name, address, gender, photo and date of birth details of the Aadhaar number holder.
(d) Aadhaar paperless offline e-KYC which is an XML document generated by UIDAI and digitally signed by UIDAI carrying name, address, gender, photo and date of birth details of the Aadhaar number holder.

B) In case, Officially Valid Documents (OVDs) furnished by the customer does not contain updated address, the following documents or the equivalent e-documents thereof shall be deemed to the OVDs for the **limited purpose of proof of address**:
(i) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
(ii) property or Municipal tax receipt;
(iii) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

(iv) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;
(The Client shall submit updated Officially Valid Document with current address within a period of three months of submitting the above document)

C) 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 shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

4.16 Offline verification means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations, as in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

4.17 Principal Officer means an officer, duly appointed by the BOD, responsible for furnishing information as per rule 8 of the Rules to FIU- IND.
The name, designation and address of the Principal Officer shall be communicated to the FIU-IND. The Principal Officer shall be independent and report directly to the senior management or to the Board of Directors. He is responsible for monitoring KYC/AML compliance at operational units, escalation of suspicious transactions reported by branches through STRs and sharing of information as required under the law. The Principal Officer and other appropriate staff shall have timely access to customer identification data and other CDD information, transaction records and other relevant information. The Principal Officer under PML Act, 2002 shall be the competent authority for fixing the thresholds for generation of AML alerts and the periodicity of reviewing the alerts shall be at half yearly intervals or as and when required.

4.18 Person 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 of the preceding sub-clauses, and
g. any agency, office or branch owned or controlled by any of the above persons mentioned in the preceding sub-clauses.

4.19 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.

It is likely that in some cases transactions are abandoned/ aborted by customers on being asked to give some details or to provide documents. Bank shall report all such attempted transactions in STRs, even if completed by the customers, irrespective of the amount of the transaction.

4.20 Small Account means a savings account in which:

a. the aggregate of all credits in a financial year does not exceed Rs.1,00,000/-;
b. the aggregate of all withdrawals and transfers in a month does not exceed rupees Rs.10,000/- and
c. the balance at any point of time does not exceed rupees Rs.50,000/-.

This limit on balance shall not be considered while making deposits through Government grants, welfare benefits and payment against procurements. Person who wants to open an account and is not able to produce any of the OVDs or the documents applicable in respect of simplified procedure, the bank shall open a small account. The account can be opened by production of a self-attested photograph and affixation of signature or thumb impression, as the case may be, on the Account Opening form. The designated branch official, while opening the small account, should certify under his signature that the person opening the account has affixed his signature or thumb impression as the case may be, in his presence. The account shall 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. The entire relaxation provisions shall be reviewed after twenty four months.

4.21 Transaction: means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes –

a. opening of an account;
b. deposits, withdrawals, 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 a part of any contractual or other legal obligation;
f. establishing or creating a legal person or legal arrangement.

4.22 Money Laundering is a process by which money or other assets obtained illegally are exchanged for "clean money" or other assets with no obvious link to their criminal origins. Individuals with criminal intent, resort to Money Laundering to disguise the true origin of the proceeds of criminal activities through the financial system so that after a series of transactions, the money, its ownership and the income earned from it appear to be legitimate.

The 3 common stages of money laundering are given below:

a. Placement-the physical disposal of cash proceeds derived from illegal activities
b. Layering-separating illicit proceeds from their source by creating complex layers of

financial transactions designed to disguise the source of money, subvert the audit trail and create anonymity;

c. Integration-creating the impression of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds.

Money Laundering Prevention is not only a statutory or regulatory requirement but also a moral responsibility for the Bank employees as any facilitation of money laundering indirectly supports these criminal activities.

*The **Prevention of Money Laundering Act, 2002 (PMLA)** Act & Rules is India's legislation for combating money laundering. The objective of this Act is to prevent money laundering and to provide for confiscation of property derived for or involved in money laundering.*

Section 3 of the PMLA criminalises the activity of money laundering as follows:
"Whoever, directly or indirectly, attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering."
"Proceeds of crime"is the property derived directly or indirectly as a result of criminal activity relating to an offence included in the Schedule to PMLA.

4.23 Terrorist Financing

Terrorists use similar methods as Money Launderers for moving their funds. Some of the terrorist groups also indulge in criminal activities for generating funds for their activities and some of them are even known to have strong relationships with criminal gangs. The two major differences between terrorist financing and money laundering are:

- Terrorist funding can happen from legitimately obtained income whereas the source of money in money laundering is always from illegal source, and
- More often terrorist activities require small amounts and hence it is increasingly difficult to identify terrorist funding.

*The **Unlawful Activities (Prevention) Act, 1967 (UAPA)** is India's legislation to combat terrorism and its financing. UAPA criminalises terrorist acts and raising of funds for terrorist acts and the penal provisions of UAPA are laid down under sec 17 & sec 40 of the Act.*

UAPA also provides for freezing / un-freezing of Assets under section 51 A (refer Procedure).

RBI circulates the designated list to Banks who have to check whether any of the names match to any existing customers holding Bank accounts. In case of any matching details, the Bank has to inform

- *Ministry of Home affairs within 24 hrs.*
- *UPA Nodal Officer of RBI,*
- *UAPA's nodal officer of the state / UT*
- *file STR with FIU –IND*

Combating Financing Of Terrorism: In terms of PMLA, the Bank should have a suitable mechanism to identify & monitor accounts & transactions suspected of having terrorist links, report to (FIU-India) on priority. List of suspect individuals / entities received from RBI / UNSCR to be circulated to Branches & scrutinized.

Branches are advised before opening any new account it should be ensured that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/ entities in the list should be immediately intimated to RBI and FIU-IND. The Bank will also file a Suspicious Transaction Report (STR) as per the prescribed format with FIU-IND covering all transactions in the accounts covered above.

4.24 Video based Customer Identification Process (V-CIP)

It 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.

4.25 Other Terms: Following Terms shall 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. **Walk-in Customer** means a person who does not have an account based relationship with the Bank but undertakes transactions with the Bank.
iii. **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.
iv. **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.
v. **KYC Templates** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
vi. **Non-face-to-face customers** means customers who open accounts without visiting the branch/offices of the Bank or meeting the officials of the Bank.
vii. **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.
viii. **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.
ix. **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.
x. **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.
xi. **Wire transfer** means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank.

xii. **Domestic and cross-border wire transfer**: When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the 'originator bank' or 'beneficiary bank' is located in different countries such a transaction is cross-border wire transfer.

All other expressions unless defined herein shall 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, 2022 and 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 thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

5. POLICY BACKGROUND

International Developments & Regulatory requirements

5.1 Financial Action Task Force (FATF)

FATF is an independent inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction, and other related threats to the integrity of the international financial system.

The FATF Recommendations are the basis on which all countries should meet the shared objective of tackling money laundering, terrorist financing and the financing of proliferation. The FATF calls upon all countries to effectively implement these measures in their national systems. India is a member of the FATF.

5.2. United Nations Security Council Resolutions (UNSCR)

These UN Security Council Resolutions require members to take steps in preventing terrorism and UN issues lists of names of persons and organizations concerned with terrorism and the member countries are required to freeze their assets. These lists are periodically downloaded by the Bank and circulated across branches for scrutinizing their accounts and reporting to authorities.

5.3 Legislations & Regulations in India

Legislations:

Prevention of Money Laundering Act, 2002 (PMLA) Act & Rules
Prevention of Money Laundering (Amendment) Act, (PMLA) 2009.
The Unlawful Activities (Prevention) Act, 1967 (UAPA)
Foreign Account Tax Compliance Act (FATCA) & Common Reporting Standard (CRS)

Regulations:

AML: Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), Insurance Regulatory and Development Authority (IRDA) and FIU-IND are the bodies mainly responsible for the anti-money laundering efforts for financial institutions in India. RBI is the lead regulator for banks and other financial institutions issue regulations on the subject. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister of India and is responsible for receiving, processing, analyzing and

disseminating information relating to suspicious financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and related crimes.

FATCA CRS: In 2010, USA enacted a law known as "Foreign Account Tax Compliance Act" (FATCA) with the objective of tackling tax evasion through obtaining information in respect of offshore financial accounts maintained by USA residents and citizens.
Under FATCA and CRS, the Bank shall 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.
India has signed the Inter-Governmental Agreement (IGA) with the USA on July 9, 2015, for Improving International Tax Compliance and implementing the Foreign Account Tax Compliance Act (FATCA). India has also signed a multilateral agreement on June 3, 2015, to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters under the Common Reporting Standard (CRS), formally referred to as the Standard for Automatic Exchange of Financial Account Information (AEOI). In this regard, Government of India has notified the amendments to Income Tax Rules (Rules) for operationalisation of IGA and CRS. This information regarding US reportable persons and other reportable persons have to be furnished in a form 61B, which has also been notified with the above mentioned notification.
The Bank being a Reporting Financial Institution has registered itself as a Depository institution and have to report both depository and custodial accounts held by us.

The key circulars on which this policy document is based are:

- Master Direction-Know Your Customer (KYC) Direction, 2016 (Updated as on May 10, 2021).
- UN Security Council Resolutions 1267 (1999) - RBI Circulars issued from time to time.
- Guidelines on detecting suspicious transactions under Rule 7(3) of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 for Cooperative Banks.
- IBA Guidance Note on KYC/ AML dated July 2009.
- IBA-Implementation of Red Flag Indicators, 2012.

6. POLICY FRAMEWORK AND MECHANISM

6.1 Implementation of KYC / AML / CFT regime in the Bank

All employees shall be fully aware of the risks to bank management posed by the abuse of financial services by organized crime, including money laundering and terrorist financing. Additionally, all employees shall, consistent with their job responsibilities, be required to play an active role in anti-money laundering measures, including this Policy, towards preventing the improper use of the financial services provided by the Bank.

The key elements of KYC Policy are:

a. Customer Acceptance Policy
b. Risk Management
c. Customer Identification Procedures
d. Monitoring of Transactions

6.2. Customer Acceptance Policy (CAP)

i) No account will be opened in anonymous or fictitious/ benami name (s)

ii) No account will be opened where the Bank is unable to apply appropriate Customer Due Diligence (CDD) measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

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

iv) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is obtained.

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

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

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

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

ix) The Bank shall have the option of establishing a relationship with PEPs provided that instructions contained under Enhanced Due Diligence for Accounts of Politically Exposed Persons is adhered to (Refer Pt. 6.7).

x) Name Screening to be carried out 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.

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

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

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

6.2.1 Name screening

Name screening refers to the process of determining whether any of the bank's existing or potential customers are part of any blacklists or regulatory lists. As part of the Customer Acceptance Policy the Bank makes it mandatory that before opening a new account so as to ensure the identity of the customer does not match with any person with known criminal background or with banned entities such as terrorist individuals or terrorist organizations, name screening process is performed for the following types of transactions:

- New customers should be screened at the time of opening of accounts.
- Screening of legacy customers, i.e. screening of the bank's existing customers at regular intervals.
- Employees are required to be screened as a part of their pre-recruitment process, besides screening the existing employees at regular intervals.
- Counter parties to the cross border transactions (i.e. remitters, beneficiaries, intermediary banks, other intermediaries, etc.) in remittance or trade transactions need to be screened.
- It also needs to be a part of the enhanced due diligence for high-risk customers or suspicious transactions review.

The nature and extent of due diligence will depend on the risk perceived. Care to be taken to

seek only such information from the customer, which is relevant to the risk category and is not intrusive.

However adoption of customer acceptance policy and its implementation should not become too restrictive and must not result in denial of banking services to general public, especially to those, who are financially or socially disadvantaged.

Requirements/Obligations under International Agreements

Communications from International Agencies –

Bank / Branch / CPD shall ensure that 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:

(a) The **"ISIL (Da'esh) & Al-Qaida Sanctions List"**, which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at *https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl*

(b) **The "1988 Sanctions List",** consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at *https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl.*

Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under Unlawful Activities (Prevention) Act, 1967 (UAPA) notification dated February 02, 2021 (Annex II of the RBI Master Direction, 2016 – Updated on 10.05.2021).

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

Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

The procedure laid down in the UAPA Order dated February 2, 2021 (Annex II of the RBI Master Direction, 2016 – Updated on 10.05.2021) 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 Ministry of Home Affairs.

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, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.

b. Special attention shall 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 Point 9.2 a & b under Secrecy Obligations and Sharing of information does not preclude the 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 shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.

6.2.2 Unique Customer Identification Code (UCIC) for customers

The Bank has allotted UCIC to all its new customers, to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and have a better approach to risk profiling of customers.

The increasing complexity and volume of financial transactions necessitate that customers do not have multiple identities within a bank, across the banking system and across the financial system. UCIC helps the bank to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and to have a better approach to risk profiling of customers.

6.3 Risk Management

Customers shall be categorized as low, medium and high risk category, based on the assessment. Risk categorization shall be undertaken based on parameters such as customer identity, social/financial status, nature of business activity and information about the customer's business and their location etc.

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

The Board of Directors have ensured that an effective KYC and AML Policy is put in place by establishing appropriate procedures and their effective implementation.

Proper internal controls are maintained by allocating specific duties and responsibilities to the Bank's staff to ensure accountability about strict compliance of the guidelines of the KYC and AML Policy.

The Internal Audit/ Inspection teams of the Bank are authorised to make an independent evaluation of the internal control, including legal and regulatory requirements exercised by the CPD Account Opening Unit (AOU) / branches to implement the KYC and AML Policy of the Bank and make suitable comments thereon in their Audit/Inspection reports. Similarly, the Concurrent /Internal Auditors are empowered to scrutinize and comment upon the effectiveness of the measures taken by the branches & CPD – AOU for adoption of the Bank's KYC Policy. Compliance Reports by the Internal/ External Auditors are placed before the Audit Committee of the Board at quarterly intervals.

6.3.1 Customer profiling

The Customer Profile will contain information relating to customer's identity, social/ financial status, nature of business activity, information about his clients' business and their location etc. The newly introduced Account Opening form has a Customer Identification Form (CIF) which will enable Customer profiling for new customers. The CIF for existing customers will enable Customer profiling & Risk Categorization into High-Medium –Low Category & the same to be updated in the system.

6.3.2 Risk Categorization

'Customer risk' in the present context refers to the **money laundering risk or terrorist financing risk** associated with a particular customer from a bank's perspective. This risk is based on the risk perceptions associated with the parameters comprising a customer's profile, and the level of risk associated with the product and channels being used by him. Accordingly, the Bank

categorizes customers into low, medium, & high risk categories and has differential due diligence and monitoring standards based on the risk assessment.
Every Customer Id linked to an account should be risk categorized as 'Low", "Medium" or "High" excluding closed accounts. Risk Categorization of a customer has to be uniform throughout i.e. SB, CD, TD or LN to be classified a specific risk category only and shouldn't differ.

Risk Categorization of the customers shall be done according to the risk perceived while taking into account the following factors:
(i) Customer risk: Determine risk based on customer profile, Constitution, nature of business, occupation financial status etc.
(ii) Countries/Geographic risk: Determine risk based on residential status/location of the customer, country of nationality
(iii) Product/Service risk: Determine risk based on the product or services offered.
(iv) Transactions: Determine risk based on nature of transactions-High turnover transactions, predominantly cash transactions, credit turnover
(v) Reported STR/CTR/NTR/CCR

Risk Categories:

a) Low Risk Customers – Individual (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 (e.g.)

- Salaried employees – whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover.
- Government departments & Government owned companies, regulators and statutory bodies etc.

Only the basic requirement of verifying the identity and location of the customer are to be met.

b) Medium or High risk customers – Customers that are likely to pose a higher than average risk depending on customer's background, nature and location of activity, country or origin sources of funds and client profile etc. Due Diligence is required for higher risk customers, especially those for whom the sources of funds are not clear (e.g.).

- Non – Resident customers.
- High Net Worth individuals/entities
- Trusts, Charities, NGOs and organizations receiving donations.
- Cash intensive businesses, accounts of bullion dealers (including sub dealers) and jewelers.
- Companies having close family shareholding or beneficial ownership.
- Firms with 'sleeping partners'
- Politically Exposed Persons (PEPs) i.e. individuals who have been entrusted with prominent public functions in a foreign country.
- Non-face to face customers.
- Those with dubious reputations as per public information available etc.
- Customers who fall under "high risk" geographies
- Defaulters to be classified as high risk.

Risk categorization of **new customers at the time of onboarding to be based on occupation, constitution, residential status, nature of business, country of nationality, source of funds**

etc.

Periodic Review of Risk Categorization

The Bank has a system of periodical review of risk categorization of accounts once in six months. Review of Risk categorization of customers is to be done at half yearly intervals as on the **31st March** and as on **30th September** each year. The review of risk categorisation will be conducted centrally through the system based on set parameters.

6.3.3 Money Laundering and Terrorist Financing Risk Assessment

(a) Bank shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

The 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, Banks shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with REs from time to time.

(b) The risk assessment by the Bank shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Bank. Further, the periodicity of risk assessment exercise shall be determined by the Board of the Bank, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

(c) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies.

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

6.4 Customer Identification Procedure (CIP)

"**Customer identification**" means undertaking the process of CDD. The Bank shall 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 the 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. Introduction is not to be sought while opening accounts

6.5 Customer Due Diligence (CDD)

CDD means identifying and verifying the customer and the beneficial owner.

- The Bank should identify the customer and verify his/her identity by using reliable, independent source document, data or information.
- For customers that are natural persons the bank should obtain sufficient identification data to verify the identity of the customer, his address/ location and recent photograph.
- For customers that are legal persons or entity, the bank should verify the legal status of the legal person/ entity through proper and relevant documents, any person purporting to act on behalf of the entity is authorized to do so and identify and verify the identity of such person, understand the ownership and control structure of the entity and determine who are the natural persons who ultimately control the legal person.
- KYC verification once done by one branch/office of the Bank shall be valid for transfer of the account to any other branch/office of the same Bank, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation

6.5.1 CDD for Individuals

For undertaking Customer Due Diligence (CDD), Bank shall obtain the following from an individual (Refer Annexure 13.1) while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:

(A) The Aadhaar number where,

(i) he 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 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; 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) One recent photograph; and

(D) Atleast one document or the equivalent e-document thereof in support of the declared Profession / activity, nature of business or financial status, annual income, turnover (in case of business) such as salary slip, Registration certificate, Certificate / licence issued by the municipal authorities under Shop and Establishment Act, Sales and income tax returns, CST / VAT / GST certificates, Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, Licence / certificate of practice issued by any professional body incorporated under a statue, Complete Income Tax Returns (Not just the acknowledgement) etc. However, customers who don't have business / financial activity or don't have any proof in this regard such as housewife, student, minor, labour working in un-organized sector, farmers etc may submit self-declaration to this effect.

Provided that where the customer has submitted,

i) **Aadhaar number** under clause (A) above to a bank, such bank shall carry out authentication of the customer"s Aadhaar number using **e-KYC authentication** facility provided by the UIDAI. 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 (B) above **where offline verification can be carried out, the bank shall carry out offline verification.**
iii) An equivalent **e-document** of any OVD, the bank shall **verify the digital signature** as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Annexure 13.3.
iv) **Any OVD or proof of possession of Aadhaar number** under clause (C) above **where offline verification cannot be carried out**, the bank shall carry out verification through **digital KYC** as specified under Annexure 13.3.

Provided that **for a period not beyond such date** as may be notified by the Government for a class of Regulated entities, **instead of carrying out digital KYC**, the Regulated entity 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, Banks shall, 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 shall invariably be carried out by an official of the Bank and such exception handling shall also be a part of the concurrent audit. The bank shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall 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 shall be subjected to periodic internal audit/inspection by the Bank and shall be available for supervisory review.

Note:

a) Bank shall, 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** under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act
b) Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators.
c) The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act 2016 and the regulations made thereunder.
d) In case OVD furnished by the client does not contain updated address, certain deemed OVDs for the limited purpose of proof of address can be submitted provided that the OVD updated with current address is submitted within 3 months.
e) For existing bank account holders, PAN or Form No. 60 is to be submitted within such timelines as may be notified by the Government, failing which account shall be subject to temporary ceasing till PAN or Form No. 60 is submitted. However, before temporarily ceasing operations for an account Bank shall give the customer an accessible notice and a reasonable opportunity to be heard.

6.5.2 CDD for Sole Proprietary firms

For opening an account in the name of a sole proprietary firm,

i. CDD of the individual (proprietor) as detailed in Annexure 13.1 shall be carried out
ii. In addition to the above, any two of the documents as a proof of business/ activity in the name of the proprietary firm as detailed in Annexure 13.2 shall also be obtained
iii. In cases where the Bank is satisfied that it is not possible to furnish two such documents, the bank may, at its discretion, accept only one of the stipulated documents as proof of business/activity, provided **contact point verification** is undertaken and collects such other information and clarification as would be required to establish the existence of such firm is collected, to confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

6.5.3 CDD for Legal Entities

For opening an account of a legal entity (**company, partnership firm, trust, unincorporated association or body of individuals, HUF, juridical persons**)

1. Certified copies of each of the documents or the equivalent e-documents thereof stated in Annexure 13.2 shall be obtained:
2. Any such other documents pertaining to the nature of business or financial status

For non-individual customers, PAN/Form No. 60 of the entity (for companies and Partnership firms – only PAN) shall be obtained apart from other entity related documents. The PAN/Form No. 60 of the authorized signatories shall also be obtained.

6.5.4 CDD for Beneficial Owner

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

i. Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.
ii. 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 shall be obtained.

6.5.5 CDD for Basic Savings Bank Deposit Accounts (BSBDA)

i. BSBDA (General)

CDD as stipulated for Individuals in Annexure 13.1 to be undertaken for opening normal BSBDA account. There is no relaxation in KYC requirement.

ii. For BSBDA Small accounts:-

This facility is introduced in order to extend banking services and financial inclusion of a large number of persons especially those belonging to low income group both in urban and rural areas who are not able to produce documents to satisfy the Bank about their identity and address.

In case an individual customer who does not possess any of the OVDs and desires to open a bank account, banks shall 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 shall not be considered while making deposits through Government grants, welfare benefits and payment against procurements.

Further, small accounts are subject to the following **conditions**:

i. A **self-attested photograph** of the customer to be obtained
ii. 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 shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature and the account shall remain operational on annual submission of certificate of proof of address issued by the officer in-charge of the jail.
iii. Banks shall 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.
iv. The account shall 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.
v. The entire relaxation provisions shall be **reviewed after twenty four months**.
vi. Notwithstanding anything contained in clauses (iv) and (v) above, the small account shall remain operational between April 1, 2020 and June 30, 2020 and such other periods as may be notified by the Central Government.
vii. The account **shall 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 shall be established through the production of an OVD and Permanent Account Number or Form No.60, as the case may be.
viii. **Foreign remittance shall not be allowed** to be credited into the account unless the identity of the customer is fully established through the production of an OVD and Permanent Account Number or Form No.60, as the case may be.

6.5.6 CDD for Minor accounts

Operated by Guardian

- CDD for individuals to be undertaken for the Guardian
- Copy of Municipal Birth certificate/identity proof/identity card and photograph of the minor.

Operated independently by minor (Junior A/c)

A savings bank account can be opened and operated by a minor (aged 10-18 yrs) independently only if he/she can sign and is literate. Basic KYC norms to be followed:

- Recent photograph
- Copy of Aadhar card/OVD where the date of Birth is mentioned. If not available, Municipal Birth certificate/School ID card with DOB to be provided.
- Introduction / Declaration from parents for operation of account and confirming KYC details
- CDD of the Guardian

On attaining majority the erstwhile minor should confirm the balance in his/her account and fresh operating instructions and KYC documents to be obtained.

6.5.7 CDD for Non-Resident Individuals

(Non-Resident Indian (NRI), Person of Indian Origin (PIO) *and Overseas Citizen of India (OCI))*

I. OVD (proof of Identity & Indian address) for NRI / PIO / OCI: Any one of the following

- the passport,
- the driving licence,
- proof of possession of Aadhaar number,
- the Voter's Identity Card issued by the Election Commission of India,

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 shall be accepted as proof of address.

II. Non-Resident Status Proof

NRI

- Photocopy of Valid Employment/Residence/Student/Dependent visa copy or work/Residence Permit Copy/**CDC document in case of seafarers**

PIO/OCI

- Photocopy of OCI (Overseas Citizen if India) card / PIO (Person of Indian Origin) card/PIO Declaration wherever Applicable
- Copy of relevant pages of passport of parents or grandparents/ Copy of Marriage certificate-if spouse of Indian citizen

III. Proof of Overseas Address (mandatory): Any one of the following

- Valid Passport
- Overseas Driving License
- Any other document as notified by the Central Government in consultation with the regulator
- Utility bill (Electricity / Telephone / Post-Paid Mobile Phone / Piped Gas / Water Bill) - (not more than 2 months old)
- Property or Municipal Tax Receipt
- Bank Account / Credit Card or Post Office Savings Bank Account statement (not more than 3 months old)
- Pension or Family Pension Payment Orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address
- Letter of allotment of accommodation / Leave and License agreements allotting official accommodation from employer issued by State or Central
- Govt. departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies.
- Document issued by Government Department of Foreign Jurisdiction (Work/Resident Permit, Social Security Card, Green Card etc.)
- Letter issued by Foreign Embassy or Mission in India

IV. FATCA CRS Self Declaration form (mandatory): For the form to be valid, it must be dated, signed and include the Account Holder's: name; residence address; jurisdiction(s) of residence for tax purposes; TIN(s) and date of birth.

V. Mandatory documents/details

- Copy of PAN/Form 60 (in absence of PAN)
- Photocopy of Valid Indian/Foreign passport with name, address, photograph, signature, date of birth, date and place of issue, expiry date and stamp regarding stay outside India
- Latest passport size photograph
- Email address and Contact number to be taken.

Please note that:

- All documents are to be Self-Attested (all copies)
- In case the customer is physically present at the time of account opening, verification with originals is to be done by the staff present at the Branch.
- In case the customer is not physically present at the time of account opening, the original certified copy of OVD, 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.

- In case the documents given are not in English, then a duly notarised translated copy in English to be obtained

6.5.8 Account opened using OTP based e-KYC, in non-face-to-face mode

The bank may open accounts using OTP based e-KYC in non-face-to-face mode subject to the following conditions

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

(ii) 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.

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

(iv) 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.

(v) Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per CDD standards for individuals (Pt. 6.5.1) or as per V-CIP (Pt.6.5.10) is carried out. If Aadhaar details are used under V-CIP, the process shall be followed in its entirety including fresh Aadhaar OTP authentication

(vi) 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.

(vii) 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 Regulated Entity. Further, while uploading KYC information to CKYCR, the bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other REs shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

(viii) The 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.

6.5.9 Accounts of non-face-to-face customers (Other than Aadhaar OTP based on-boarding)

Bank shall ensure that the first payment is to be effected through the customer's KYC-complied account with another bank, for enhanced due diligence of non-face-to-face customers.

6.5.10 Video Based Customer Identification Process (V-CIP)

The Bank may undertake 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, Banks shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, apart from undertaking CDD of the proprietor.

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

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

V-CIP is to be carried by a Bank Official after obtaining the customer's informed Consent.

Banks opting to undertake V-CIP, shall adhere to the following minimum standards

a) V-CIP Procedure:

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

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

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

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

v) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list 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 56, using the KYC identifier provided by the customer
   d. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker

Banks shall ensure to redact or blackout the Aadhaar number as specified under CDD for

Individuals.

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

Further, in line with the prescribed period of three days for usage of Aadhaar XML file / Aadhaar QR code, REs shall ensure that the video process of the V-CIP is undertaken within three days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. However, Banks 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 banks take help of Banking Correspondents (BCs) facilitating the process only at the customer end. Banks 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.

b) 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. Banks 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 MD, 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.

c) V-CIP Infrastructure to be in place as stipulated in the RBI Master Directions on KYC.

6.6 Ongoing Due Diligence

6.6.1 Monitoring of Transactions

Bank shall 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.

i. Without prejudice to the generality of factors that call for close monitoring following types of transactions shall 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.

ii. The extent of monitoring shall be aligned with the risk category of the customer. High risk accounts have to be subjected to more intensified 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 shall be put in place.
   b. The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

Explanation: Cases where a large number of cheque books are sought by the company and/or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.'

6.6.2 Periodic KYC Updation

Bank shall adopt a risk-based approach with respect to periodic updation of KYC. 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. Policy in this regard shall be documented as part of the Bank's internal KYC policy duly approved by the Board of Directors or any committee of the Board to which power has been delegated. Further to amendment to RBI Master Direction on KYC dated 10.05.2021, it may be noted that during activation of inoperative accounts or periodic KYC in all categories of accounts, fresh KYC documents need not be taken unless there is change in KYC information.

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, letter, or in person 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, letter, or in person 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, if the current address/mailing address provided by the customer/recorded in the system does not match with the address in the OVD provided by the customer, then a fresh OVD with the current address is to be submitted. The documents are to be self-attested by the customer and verified from original by the Branch staff.

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. Fresh KYC may be obtained if not available with the Bank.

b) Customers other than individuals/Legal Entity (LE):

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, letter from an official authorized by the LE in this regard, board resolution etc.

Further, the Bank shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.

ii. **Change in KYC information:** In case of change in KYC information, the 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, the Bank shall ensure that,

i. The KYC documents of the customer as per the current CDD standards are available with them. 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 details, if available with the Bank, is verified from the database of the issuing authority at the time of periodic updation of KYC.

iii. Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of the Bank and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

iv. In order to ensure customer convenience, the facility of periodic updation of KYC will be made available at any branch.v. The Bank shall adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, which otherwise are not mandated under the above instructions, adopted by the Bank such as requirement of obtaining recent photograph, requirement of physical presence of the customer, requirement of periodic updation of KYC only in the branch of the Bank where account is maintained, a more frequent periodicity of KYC updation than the minimum specified periodicity etc., shall be clearly specified in the internal KYC policy duly.

vi. The Bank shall ensure that the internal 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.

6.6.3 Obtention of PAN/Form 60

i. In case of existing customers, the Bank shall 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 the Bank shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-document thereof or Form No. 60 is submitted by the customer. Here, particularly in this context, "temporary ceasing of operations" in relation an account shall 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 shall be allowed.

ii. Provided that before temporarily ceasing operations for an account, the bank shall give the client an accessible notice and a reasonable opportunity to be heard. Further, appropriate relaxation(s) 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 will be given. Such accounts shall, however, be subject to enhanced monitoring.

iii. Provided further that if a customer having an existing account-based relationship with a 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 shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

6.7 Enhanced Due Diligence Procedure

6.7.1 Accounts of Politically Exposed Persons (PEPs)

The Bank shall 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 shall have been verified before accepting the PEP as a customer;
c) the decision to open an account for a PEP is taken after reference to Operations Dept
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, CAO approval is obtained to continue the business relationship;
f) the CDD measures as applicable to PEPs include enhanced monitoring on an on-going basis

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

6.8 Simplified Due Diligence

6.8.1 Simplified norms for Self Help Groups (SHGs)

a. CDD of all the members of SHG shall not be required while opening the savings bank account of the SHG.
b. CDD of all the office bearers shall suffice.
c. Customer Due Diligence (CDD) of all the members of SHG may be undertaken at the time of credit linking of SHGs.

7. REPORTING REQUIREMENTS

Reporting of suspicious transactions are done by the Branches to the Central Office which screens all alerts and identifies the Suspicious Transactions to the Principal Officer. The Bank is required to upload the following digitally signed reports to the FIU- IND on the Finnet portal.

7.1 Reporting requirements under PMLA Act

7.1.1 Cash Transaction Report (CTR)

The Prevention of Money Laundering Act, 2002, and Rules thereunder require every banking company, financial institution and intermediary, to furnish to FIU-IND information relating to -

- All cash transactions of **value of more than Rupees Ten Lakhs or its equivalent in foreign currency.**
- All series of cash transactions integrally connected to each other which have been individually valued below Rupees Ten Lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds Rupees Ten Lakhs or its equivalent in foreign currency.

7.1.2 Suspicious Transactions Report (STR)

Every banking company, financial institution and intermediary shall furnish to FIU-IND information of all suspicious transactions whether or not made in cash.

Suspicious transaction means a transaction refers to an attempted transaction, whether or not made in cash which to a person acting in good faith-

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

Broad categories of reason for suspicion and examples of suspicious transactions are indicated as under:

Identity of client

- False identification documents
- Identification documents which could not be verified within reasonable time
- Accounts opened with names very close to other established business entities

Background of client

- Suspicious background or links with known criminals

Multiple accounts

- Large number of accounts having a common account holder, introducer or authorized signatory with no rationale
- Unexplained transfers between multiple accounts with no rationale

Activity in accounts

- Unusual activity compared with past transactions
- Sudden activity in dormant accounts
- Activity inconsistent with what would be expected from declared business
- Unexplained travel to different branches to operate account located in a single branch

Nature of transactions

- Unusual or unjustified complexity
- No economic rationale or bonafide purpose
- Frequent purchases of drafts or other negotiable instruments with cash
- Nature of transactions inconsistent with what would be expected from declared business
- Matching in & out-immediate withdrawals being made after depositing cheques/cash

Value of transactions

- Value just under the reporting threshold amount in an apparent attempt to avoid reporting
- Value inconsistent with the client's apparent financial standing

Disclosure of STR:

- Branches shall process the alerts generated in the FINAML system on a daily basis.
- Marking of an account for disclosure has to be authorised by only the Branch Head in the FINAML software and hence the same has to be posted by the Officer assigned under the Branch Head.
- The Branch Head shall forward a mail to the Group immediately on disclosing an account as suspicious in the FINAML software along with detailed reasoning and due diligence taken by the Branch to report the account as suspicious. The detailed reasoning & due diligence for reporting an account as suspicious should include the reason for finding the transactions as suspicious, the investigation carried out by the Branch, that includes inquiry conducted, field visits, the occupation/nature of business and the KYC Compliance of the customer (Refer Annexure 13.7).
- On receipt of mail from the Branch, the Groups should confirm the suspicious nature of the alert disclosed by the Branch taking necessary due-diligence. If found suspicious, the same to be escalated by the respective Group Head to the Compliance Department for further action. If the ground of suspicion is not found reasonable by the Group the same to be conveyed to the Branches and the alert to be closed as False/Positive accordingly.
- On confirmation of the suspicious nature of transaction/activity from the Group Head, the Compliance Dept. shall further carry out necessary due diligence and report the said account as STR to FIU-India if found suspicious.

7.1.3 Counterfeit Currency Report (CCR)

The Prevention of Money Laundering Act, 2002, and Rules thereunder require every banking company, financial institution and intermediary, to furnish to FIU-IND information relating to all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions.

7.1.4 Non-Profit Organisation Transaction Report (NTR)

The Prevention of Money Laundering Act, 2002, and Rules thereunder require every banking company, financial institution and intermediary, to furnish to FIU-IND information relating to all transactions involving **receipts by non-profit organisations of value more than rupees ten lakh,** or its equivalent in foreign currency. Branch to ensure that all NPOs with heavy transactions should be KYC compliant & that the transactions in the account matches the profile of the customer.

7.1.5. Due Date for Filing Reports

CTR, NTR, CCR – due by 15th of the succeeding month

STR – seven working days on being satisfied that the transaction is suspicious

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

Under FATCA and CRS, the Bank has registered as a Reporting Financial Institution as defined in Income Tax Rule 114F.

a. Bank shall 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) shall be referred to.
Explanation: Bank shall 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.
b. Develop Information Technology (IT) framework for carrying out due diligence procedure and for recording and maintaining the same, as provided in Rule 114H.
c. Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules.
d. Constitute a "High Level Monitoring Committee" under the Designated Director or any other equivalent functionary to ensure compliance.
e. 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

7.2.1 Due diligence to be taken while accepting FATCA CRS forms from customers

- Occupation of the customer to be obtained on the self-declaration form.
- Foreign Address to be mandatorily mentioned under Current residence for non-resident customers
- Residence for Tax purposes will be the foreign address only for non-residents unless he/she is a seafarer or student
- A person can be resident for tax purposes in more than one country and have more than 1 TIN/Functional equivalent.
- If the customer has not mentioned his TIN/Functional equivalent, then he/she **must** mention the reason for the same under Part II c of the FATCA CRS form.
- Ensure Continuous Discharge Certificate (CDC) is obtained for seafarers is not taken.
- Ensure that the FATCA CRS self –declaration forms are duly filled and valid. For the form to be valid, it must be dated, signed and include the Account Holder's: name; residence address; jurisdiction(s) of residence for tax purposes; TIN(s) and date of birth.
- Confirm the reasonableness of such self-certification based on the information obtained by it in connection with the opening of the account, including any documentation collected in accordance with Prevention of Money Laundering (Maintenance of Records) Rules, 2005.
- The CRS TIN leaflet may be referred to for detailed TIN/Functional equivalent name/description, structure, where to find TIN/Functional equivalent.

8. RECORD MANAGEMENT

A record of transactions in the account are preserved and maintained as required in terms of section 12 of the PML Act, 2002 and transactions of suspicious nature and/or any other type of transaction notified under the section 12 of the PML Act, 2002 are reported to the appropriate law enforcement authority.
Under Rule 3, proper records of all cash transactions (deposits and withdrawals) of Rs.10 lakhs and above (individual and integrally connected transactions) are maintained.
As per the Act, the Bank maintains **at least five years from the date of transaction between the bank and the client**, all necessary **records of transactions,** both domestic and international, which will permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

(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.

The Bank also ensures that **records pertaining to the identification of customer** and his address obtained while opening the account and during the course of business relationship are properly preserved for **at least five years after the business relationship is ended.**
The records mentioned may be maintained in hard or soft copy.
The following documents are to be maintained and preserved for a minimum period of five years.

- Records including identification obtained in respect of all transactions.
- Cash transactions of the value more than Rs.10,00,000 or its equivalent in foreign currency including all series of cash transactions integrally connected to each other valued below Rs.10,00,000 or its equivalent in foreign currency where such series of transactions have taken place within a month.
- All information with respect to the nature, amount of the transactions, date of the transactions and parties to the transactions are to be maintained and preserved.
- Details of all transactions involving purchase of foreign exchange against payment in cash exceeding Indian Rupees 10,00,000 from inter-related persons during one month.
- Statements/Registers prescribed by the Reserve Bank from time to time
- All Inspection/ Audit/ Concurrent Audit Reports.
- Annual Reports of the Principal Officer submitted to the Top Management.
- Details of all suspicious transactions reported in writing or otherwise to the Principal Officer.
- All correspondence/ reports with the appropriate authority in connection with suspicious transactions.
- References from Law Enforcement Authorities, including FIU, are to be preserved until the cases are adjudicated and closed.

9. OTHER INSTRUCTIONS

9.1 Operation of Bank Accounts & Money Mules

The instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimize 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."

9.2 Secrecy Obligations and Sharing of Information

a. Banks shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.
b. Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.
c. While considering the requests for data/information from Government and other agencies, banks shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.
d. The exceptions to the said rule shall be as under:
    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.

9.3 CDD Procedure & 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) The Bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.

c) The 'live run' of the CKYCR started from July 15, 2016 in phased manner beginning with new 'individual accounts'.

d) The Central Processing Department (CPD) of the Bank has been uploading the KYC data pertaining to all new individual accounts opened on or after April 1, 2017 on to CKYCR in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

e) The CPD shall **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) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the Bank shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above mentioned dates as per (d) and (e) respectively **at the time of periodic updation** (as specified in the Bank KYC Policy), or earlier, when the updated KYC information is obtained/received from the customer.

g) The Bank shall **ensure that during periodic updation, the customers are migrated to the current CDD standard.**

h) In terms of provision of Rule 9(1A) of PML Rules, the Central Processing Department (CPD) of 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.

i) Operational Guidelines for uploading the KYC data have been released by CERSAI and shall be followed by the CPD.

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

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

   i. there is a change in the information of the customer as existing in the records of CKYCR;
   ii. the current address of the customer is required to be verified;
   iii. the Bank considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

9.4 Partial freezing/Closure of accounts

a. Where Bank is unable to comply with the CDD requirements, they shall not open accounts, commence business relations or perform transactions. In case of existing business relationship which is not KYC compliant, banks shall ordinarily take step to terminate the

existing business relationship after giving due notice.

b. As an exception to the Rule, the Bank shall have an option to instead freeze the accounts of the customer.
c. RBI circular dated May 10, 2021 unquoted above guidelines and removed the clause for freezing the accounts for non-compliance of KYC.

1. The option of 'partial freezing' shall be exercised after giving due notice of 30 days' notice to the customers and reminder for further period of three months. All active / dormant accounts will be debit frozen (Partial) i.e. only credits will be allowed and debits will be disallowed to all KYC non-compliant accounts.
2. In case of non-complaint fixed deposits accounts there will be no freeze due to the auto renewal or credit of interest. Only alert is raised while closing the FDs for KYC compliance or closure of the FDs is not allowed till KYC compliance.
3. KYC non-complaint loan account will be debit freeze, though the system generated interest application is to be serviced.

i. When an account is 'partial freezing' or after 'partial freezing', the reason for non-submission of KYC is to be communicated to the account holder.
ii. The account holders shall have the option, to revive their accounts by submitting the KYC documents.

9.5 New products / technologies / services

New products / technologies / services should be offered only to fully KYC compliant customers & their customer ID should be duly updated

- Rupay ATM cards/ debit cards
- SMS alerts
- internet view only
- mobile banking
- third party products – referral services
- at par cheques
- Pre-paid Instruments (PPIs) etc.

9.6 Quoting of PAN

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

9.7 Wire transfers

Wire transfers (Cross borders / Domestic/ RTGS/ NEFT/ SWIFT etc.) transactions to be done only for KYC compliant customers.

9.8 Money Changing Activities

Money Changing Activities to be done only for KYC compliant customers.

9.9 Demat Accounts

Demat accounts will be opened only for KYC compliant customers & NDSL guidelines to be duly complied with. **In-person Verification (IPV) for all clients including joint account holders** is mandatory. **PAN is mandatory for all transactions in the securities market.** KYC Application form & supporting documents to be uploaded within 10 days from the date of execution of documents by Clients.

9.10 Correspondent Banking

Correspondent Banking relationship need to be managed taking a Risk-based approach & Know your Correspondent procedures. Bank will not enter into any relationship with shell banks.

9.11 Payment of cheques/drafts/pay orders/banker's cheques

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

9.12 Any remittance of funds

Any remittance of funds by way of demand draft, mail/telegraphic transfer/NEFT/IMPS or any other mode and issue of travelers' cheques for value of rupees fifty thousand and above shall be effected by debit to the customer's account or against cheques and not against cash payment.

10. ROLES & RESPONSIBILITIES:

Bank shall ensure compliance with KYC Policy through:

(a) 'Senior Management' for the purpose of KYC compliance includes the Directors including the Managing Director (Designated Director), the Deputy & Assistant General Managers.
(b) Allocation of responsibility for effective implementation of policies and procedures to be done by Operations Dept. with Group Offices, Branches and CPD- Account Opening Unit (AOU) .
(c) Independent evaluation of the compliance functions of Banks' policies and procedures, including legal and regulatory requirements to be done by Audit & Inspection Dept.
(d) Concurrent/ Internal audit system to verify the compliance with KYC/AML policies and procedures as per Audit Policy.
(e) Submission of quarterly audit notes and compliance to the Audit Committee.
(f) Review of position & pending compliances of Concurrent Audit as per RBI Calendar of Reviews to be done – quarterly.
(g) The Bank shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

10.1 Board and Senior Management

The Board of Directors and the senior management of the bank have the responsibility to ensure that the bank's control processes and procedures are appropriately designed and implemented, and are effectively operated to reduce the risk of the Bank being used in connection with money laundering or terrorist financing.

Managing the risk of money laundering

The senior management of the bank is required to ensure that appropriate risk-based policies are in place across different aspects of the business. The bank should adopt an approach to mitigate themselves of the risk of being used for the purposes of money laundering or terrorist financing. Senior management must be entirely engaged in the decision-making and must take ownership and accountability of the risk-based approach.

Formulation of appropriate procedures and policies to prevent money laundering

As per the RBI master circular, banks are required to formulate appropriate procedures to prevent money laundering, specifically KYC policies and procedures specifying the objective of KYC framework.

Guidance against "Tipping off"

Senior management should provide sufficient guidance to staff to ensure that the customers are not informed (i.e. tipped off) that his/her accounts are under monitoring for suspicious activities and/or that a disclosure has been made to the FIU-IND.

Reporting to the board

- KYC Compliance of accounts to be submitted to the Board quarterly.
- Updation of the KYC policy and changes made therein to be placed before the Board for their approval on an on-going basis.
- Risk categorization of customers done on half yearly basis to be reported to the Board.
- Implementation of KYC related procedures and activities to be carried out for KYC Compliance to be approved by the Board.
- Review of position & pending compliances of Concurrent Audit as per RBI Calendar of Reviews to be done – quarterly.

10.2 Designated Director

Designated Director, appointed by the Board of Directors, has to be one of the whole time Directors of the Bank. The Managing Director & Chief Executive Officer is the 'Designated Director' of the Bank. The Designated Director has the overall responsibility to ensure that the obligations of the PMLA is fulfilled. The name, designation and address of the Designated Director shall be communicated to the FIU-IND. In no case, the Principal Officer shall be nominated as the 'Designated Director'.

10.3 Managing Director & CEO

MD & CEO shall assess issues relating to KYC that have been reported by the Compliance Officer / Principal Officer - Person Responsible for the Prevention of Money Laundering in each office. They shall further determine whether to maintain the current relationship, to increase monitoring or to end the relationship with the customer reported by the Person Responsible for the Prevention of Money Laundering.

10.4 Principal Officer (PO) / Compliance Officer

Principal Officer (PO) / Compliance Officer shall be the Person Responsible for the Prevention of Money Laundering and shall be in charge of all matters regarding the prevention of money laundering. Principal Officer, appointed by the Board of Directors, will be responsible for monitoring and reporting of all transactions and sharing of information as required under the law, PMLA, i.e. furnishing of information to FIU-India.

The person will work independently, report any irregularities to the Management / Board of Directors and liaise with the Reserve Bank, enforcement agencies, banks and any other institutions which are involved in the fight against money laundering and combating financing of terrorism. It is recommended that the PO has a sufficient level of seniority within the bank and has sufficient resources, including sufficient time and (if necessary) support staff. The Principal Officer shall have reasonable access to all necessary information/ documents which would help him/ her in effective discharge of his / her responsibilities.

Responsibility of Principal Officer includes:

a) Putting in place necessary controls for detection of suspicious transactions.
b) Receiving disclosures related to suspicious transactions from the staff or otherwise.
c) Deciding whether a transaction should be reported to the appropriate authorities.
d) Training of staff and preparing detailed guidelines / handbook for detection of suspicious

transactions.

e) Preparing annual reports on the adequacy or otherwise of systems and procedures in place to prevent money laundering and submit it to the Top Management within 3 months of the end of the financial year.
f) Overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made there under, as amended from time to time.
g) Timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by Non-Profit Organisations of value more than Rupees ten lakh or its equivalent in foreign currency to FIU-IND.
h) Implementing and communicating the Board Decision, Policies as well as RBI requirements to the staff.

10.5 CPD- AOU Account Opening Unit

The CPD- AOU to ensure that all new accounts & existing customer IDs attached to new accounts are **KYC compliant as per our extant KYC Policy** & in conformity with RBI guidelines as issued from time to time. Further, the CPD- AOU dept. is also to ensure that the FATCA CRS self-declaration forms are **duly filled and valid** for all new accounts/customers. The same will be monitored by Internal Inspection department during their periodic quarterly Inspection of CPD department.

CPD functions & process flow are detailed in Circular Ref: 2015-16 / 17 dated 5th May 2015 (briefly).

a) Checking of KYC documents at the time of Account Opening, Updation, modification etc.
b) **New Customer ID** provided Customer does not have an existing customer ID.
c) Digitization of Customer Master data (documents to be stored based on Customer ID).
d) MIS reports relating to KYC from CBS.
e) All new products / services to be KYC compliant & duly updated in CBS.
f) All new customers are FATCA CRS compliant.
g) All new customers have provided PAN/Form 60 and the same is updated in CBS.
h) C-KYC Compliance of all new accounts and existing accounts at the time of periodic KYC Updation.
i) The Bank shall not open savings deposit account in the name of Government departments / bodies depending upon budgetary allocations for performance of their functions / Municipal Corporations or Municipal Committees / Panchayat Samitis / State Housing Boards / Water and Sewerage / Drainage Boards / State Text Book Publishing Corporations / Societies / Metropolitan Development Authority / State / District Level Housing Co-operative Societies, etc. or any political party or any trading/business or professional concern, whether such concern is a proprietary or a partnership firm or a company or an association and entities other than individuals, Karta of HUF and organisations / agencies listed in Schedule – I.

10.6 Branch Managers & Branch Staff

- Branch Managers should ensure overall KYC Compliance of the Branch. Branch Staff shall obtain, maintain and update the necessary KYC information on individual customers. They shall monitor customer behavior and report potentially suspicious activity, particularly activity inconsistent with the KYC information. They shall Process the alerts generated in the FINAML system on a daily basis.
- Branch Head responsible for Marking of an account for disclosure and reporting of the same in the prescribed format (Refer Annexure 13.5) to respective Group Office.
- Ensure that the FATCA CRS self –declaration forms are duly filled and valid. **For the form to**

be valid, it must be dated, signed and include the Account Holder's: name; residence address; jurisdiction(s) of residence for tax purposes; TIN(s) and date of birth.

• Confirm the reasonableness of such self-certification based on the information obtained by it in connection with the opening of the account, including any documentation collected in accordance with Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

10.7 Staff

All employees are required to read and understand the current policies and rules and regulations, and to participate in any relevant training. The staff that are interacting with customers or handling customer transactions/instructions at Branches are the Bank's strongest defense against money laundering or its weakest link.

- Every employee has an obligation to report transactions suspicious of a money laundering or terrorist financing activity. It is required to report suspicious transactions even if the employee does not know precisely what the underlying criminal activity is or whether illegal activities have occurred. The reporting of these transactions by an employee does not constitute breach of the employee's duty of confidentiality owed to customers. In addition, as per the PMLA 2002, the Bank and their officers shall not be liable to any civil proceedings against them for furnishing information on any suspicious transaction.
- Undertake adequate Customer due Diligence measures and comply with KYC norms.
- Risk Categorization of all new accounts based on set parameters.
- Review of Customer Risk Categorization on a half yearly basis.
- Filing various reports (CTR, NTR, CCR, STR) with Financial Intelligence unit-India.
- CTR/NTR Review on a monthly basis.
- Reporting of Form 61B (FATCA & CRS) on the Income Tax portal on an annual basis.
- It is equally important for the staff to keep themselves abreast with the policies and procedures relevant to their role.
- On-going employee training programme shall be put in place so that the members of staff are adequately trained in AML/CFT policy.

10.8 Internal Audit/ Internal Control /Concurrent Audit

Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures. Submission of quarterly audit notes and compliance to the Audit Committee

The Internal Audit and Internal Inspection teams within the bank are responsible to ascertain the effectiveness and efficiency of the **AML framework** of the bank. This would specifically include checking the adequacy of policies, procedures, and system support to detect suspicious and potential money laundering transactions, and the subsequent monitoring and reporting to regulators, FIU-IND and senior management (Detailed in Audit Policy). Further, ensure that the Bank is **FATCA CRS compliant** and ascertain the **reasonableness** of such self-certification based on the information obtained by it in connection with the opening of the account, including any documentation collected in accordance with Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

Concurrent Audit of the compliance to KYC-AML Policy is done for all Branches monthly / bi-monthly by scrutinising the hard / soft copies of the Account opening Forms & CIF at Branches or CPD-AOU Account Opening Unit. The report is submitted to the Branch & concerned Group Office who monitors & scrutinises the compliance. The concerned Group Office to ensure that:

- Concurrent Audits are compiled & report submitted within one month.

- Complied within next month & pending compliances followed up.
- Any Concurrent Audit report or Branch compliance, unsatisfactory compliance pending for over 2 months to be reported to Internal Audit & Inspection Dept.

10.9 Group Head & Office staff

- To ensure that Concurrent Audit of new accounts to be done to ensure that new accounts are KYC compliant
- Concurrent Audit report to be received in time
- Branch Compliance to be received in time
- Pending / unsatisfactory compliance to be reported / escalated to Internal Inspection Dept.
- Group Head to confirm suspicious nature of transaction reported by the Branch Head stating necessary due diligence carried out to the Compliance Officer/ Principal Officer.

11. HR & TRAINING

11.1 Customer Education

Implementation of KYC procedures requires us to demand certain information from customers which may be of personal nature or which have hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. There is, therefore, a need to prepare specific literature / pamphlets etc. so as to educate the customer of the objectives of the KYC programme. The branch staff needs to be specially trained to handle such situations while dealing with customers.

Specific literature/pamphlets will be prepared so as to educate the customer of the Objectives of the KYC Programme. Posters / Pamphlets on KYC from RBI may be circulated to branches / customers / put up on the website to increase customer awareness.

11.2 Employees Training

On-going employee training programme shall be put in place so that the members of staff are adequately trained in KYC / AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the Bank, regulation and related issues shall be ensured.

11.3 Employee Screening

It may be appreciated that KYC norms / AML standards have been prescribed to ensure that criminals are not allowed to misuse the banking channels. It would, therefore, be necessary that adequate screening mechanism is put in place by the Bank as an integral part of their recruitment / hiring process of personnel. In order that the banking channels are not misused, the Bank adequately screens every employee of the Bank under the KYC norms/ AML standards / CFT measures as an integral part of the recruitment process.

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

12. POLICY REVIEW

The KYC Policy would be reviewed by the Board of Directors on an annual basis or earlier, if there are significant changes in the applicable statutory and regulatory guidelines.

13. ANNEXURES

ANNEXURE 13.1 - CUSTOMER DUE DILIGENCE FOR INDIVIDUALS	
Features	**Documents**
CDD Measures for individuals	For undertaking Customer Due Diligence (CDD), Bank shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity: (A) The Aadhaar number where, (i) he 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 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; 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) One recent photograph; and (D) Atleast one document or the equivalent e-document thereof in support of the declared Profession / activity, nature of business or financial status, annual income, turnover (in case of business) such as salary slip, Registration certificate, Certificate / licence issued by the municipal authorities under Shop and Establishment Act, Sales and income tax returns, CST / VAT / GST certificates, Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, Licence / certificate of practice issued by any professional body incorporated under a statue, Complete Income Tax Returns (Not just the acknowledgement) etc. However, customers who don't have business / financial activity or don't have any proof in this regard such as housewife, student, minor, labour working in un-organized sector, farmers etc may submit self-declaration to this effect. Provided that where the customer has submitted, i) Aadhaar number under clause (A) above to a bank, such bank shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the UIDAI. 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 (B) above where offline verification can be carried out, the bank shall carry out offline verification. iii) An equivalent e-document of any OVD, the bank shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Annexure 13.3.

	iv) Any OVD or proof of possession of Aadhaar number under clause (C) above where offline verification cannot be carried out, the bank shall carry out verification through digital KYC as specified under Annexure 13.3. Provided that for a period not beyond such date as may be notified by the Government for a class of Regulated entities, instead of carrying out digital KYC, the Regulated entity 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. Officially Valid Documents (OVD) are as under: 1. Passport 2. Driving License 3. Proof of possession of Aadhaar number 4. Voter Identity Card issued by Election Commission of India 5. Job Card issued by NREGA duly signed by an officer of the State Government 6. Letter issued by the National Population Register containing details of name and address 7. Any other document as notified by the Central Government in consultation with the Regulator.
Documents deemed to be OVDs for the limited purpose of proof of address for period of three months only	Where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); ii. property or Municipal tax receipt; iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation; Provided that, the customer shall submit OVD with current address within a period of three months of submitting the documents specified above.

ANNEXURE 13.2 - CUSTOMER DUE DILIGENCE FOR LEGAL ENTITIES	
CDD Measures for Sole Proprietary firms	i. CDD of the individual (proprietor) as detailed in Annexure 13.1 ii. FATCA CRS declaration of the proprietor iii. any two of the following documents or the equivalent e-documents thereof as a proof of business/ activity in the name of the proprietary firm shall also be obtained: (a) Registration certificate (b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act. (c) Sales and income tax returns. (d) CST/VAT/ GST certificate (provisional/final). (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, landline telephone bills, etc. In cases where the Bank is satisfied that it is not possible to furnish two such documents, the Bank may, at their discretion, accept only one of those documents as proof of business/activity, provided the Branch undertakes contact point verification and collects such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.
CDD Measures for Companies / Section 8 Company under Companies Act, 2013 and Section 25 Company under Companies Act, 1956	Certified copies of each of the following documents or the equivalent e-documents thereof shall 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) CDD specified for individuals to be undertaken of the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf (f) Beneficial Ownership Declaration of the Legal entity and CDD of identified Beneficial Owner/s (g) FATCA CRS declaration of legal entity and authorised signatories
CDD Measures for Partnership firms	Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained: (a) Registration certificate (b) Partnership deed (c) Permanent Account Number of the partnership firm

	(d) CDD specified for individuals to be undertaken of the person holding an attorney to transact on its behalf (e) Beneficial Ownership Declaration of the Legal entity and CDD of identified Beneficial Owner/s (f) FATCA CRS declaration of legal entity and authorised signatories
Accounts of Limited Liability Partnership	Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained (a) LLP agreement copy (b) Incorporation document and DPIN of the designated partners (c) Certification of registration issued by the ROC (d) Resolution to open an account and power of attorney granted to authorised signatories to transact on its behalf (e) Permanent Account Number of the partnership firm (f) CDD specified for individuals to be undertaken of the person holding an attorney to transact on its behalf (g) Beneficial Ownership Declaration of the Legal entity and CDD of identified Beneficial Owner/s (h) FATCA CRS declaration of legal entity and authorised signatories
CDD measures for Trusts	Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained: (a) Registration certificate (b) Trust deed (c) Permanent Account Number or Form No.60 of the trust (d) CDD specified for individuals to be undertaken of the person holding an attorney to transact on its behalf (e) Beneficial Ownership Declaration of the Legal entity and CDD of identified Beneficial Owner/s(f) FATCA CRS declaration of legal entity and authorised signatories
CDD measures for Unincorporated Association or body of individuals Explanation: Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'. Explanation: Term 'body of individuals' includes societies	Certified copies of each of the following documents or the equivalent e-documents thereof shall 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 of the person holding an attorney to transact on its behalf and CDD of such persons. (d) Bye Laws/Constitutional document or such information as may be required to collectively establish the legal existence of such an association or body of individuals- (e) Beneficial Ownership Declaration of the Legal entity and CDD of identified Beneficial Owner/s (f) FATCA CRS declaration of legal entity and authorised signatories
CDD measures for juridical persons not specifically covered in	Certified copies of the following documents or the equivalent e-documents thereof shall be obtained: (a) Document showing name of the person authorised to act on behalf of the

the earlier such as societies, universities and local bodies like village panchayats	entity; (b) CDD specified for individuals to be undertaken of the person holding an attorney to transact on its behalf and (c) Such documents as may be required to establish the legal existence of such an entity/juridical person. (d) Beneficial Ownership Declaration of the Legal entity (e) FATCA CRS declaration of legal entity and authorised signatories
CDD measures for HUF	Certified copies of the following documents or the equivalent e-documents thereof shall be obtained: (a) CDD of the karta/existing authorised signatories (b) PAN in the name of HUF (c) Declaration from the karta and HUF letter signed by all the adult co-partners (d) HUF deed (if available) (e) Beneficial Ownership Declaration of the Legal entity and CDD of identified Beneficial Owner/s (f) FATCA CRS declaration of legal entity and authorised signatories Documentation to be vetted by Legal Dept. prior to opening of HUF accounts

ANNEXURE 13.3 - DIGITAL KYC PROCESS

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

B. The access of the Application shall be controlled by the Bank and it should be ensured that the same is not used by unauthorized persons. The Application shall 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, shall visit the location of the authorized official of the Bank or vice-versa. The original OVD shall be in possession of the customer.

D. The Bank must 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 shall put a watermark 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 shall 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 shall 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), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.

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

H. Thereafter, all the entries in the CAF shall 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/ eAadhaar 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' shall 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 shall not be used for customer signature. The Bank must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

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

K. Subsequent to all these activities, the Application shall 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 shall intimate the details regarding transaction-id/reference-id number to customer for future reference.

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

a information available in the picture of document is matching with the information entered by authorized officer in CAF.
b live photograph of the customer matches with the photo available in the document.; and
c all of the necessary details in CAF including mandatory field are filled properly.;
M. On Successful verification, the CAF shall 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 13.4 – RISK CATEGORISATION PARAMETERS

I. INDICATIVE LIST OF HIGH RISK CUSTOMERS

1. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UNSC 1267 & 1988 [2011] linked to Al Qaida & Taliban.
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 locally available or commercially available.
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 as identified by FATF from time to time.
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. Accounts of Embassies / Consulates
11. Off-shore (foreign) corporation/business
12. Non face-to-face customers
13. High net worth individuals [HNIs]
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 Orders / Travelers' Checks /Money Transmission / Check Cashing / Currency Dealing or Exchange
23. Business accepting third party checks (except supermarkets or retail stores that accept payroll checks/cash payroll checks)
24. Gambling/Casinos/gaming arcades including "Junket Operators" arranging gambling tours
25. 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).

26. Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries.
27. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
28. Customers that may appear to be Multi-level marketing companies etc.
29. Non-Bank Financial Institution
30. Stock brokerage
31. Import / Export
32. Real estate/Brokerage/Construction
33. Night clubs, Saunas, Karaoke

II. INDICATIVE LIST OF MEDIUM RISK CUSTOMERS

1. Social/Community welfare activity
2. Religious Organization
3. Financial Advisors/Consultants
4. Gas Station / Manufacture of gas & fuels
5. Car / Boat / Plane Dealership
6. Electronics (wholesale / retail)
7. Travel agency / reservation / tour operator
8. Used car sales
9. Telemarketers and marketing
10. Providers of telecommunications service, internet café, IDD call service, phone cards, phone center, call 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, mobile food service, accommodation, hotels, guest house, resorts, event management, hospitality, shopping malls, hospitals, medicals, dental clinic, labs, clinics, 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
20. Media agency, advertising, market research, broadcasting and programming
21. Civil Engineering-road, railway, utility
22. Estate/Inheritence accounts
23.
24.
25.
26. Marine & port related services
27. Mining and quarrying
28. Motion pic/Video/TV program production
29. Pharmaceuticals
30. Scrap Dealers, trader
31. Retail sale of wine/alcoholic beverages
32. Manufacture of tobacco products

III. LIST OF HIGH / MEDIUM RISK PRODUCTS & SERVICES

1. Electronic funds payment services such as Electronic cash (e.g., stored value and payroll cards), funds transfers (domestic and international), etc
2. Electronic banking
3. Private banking (domestic and international)
4. Trust and asset management services
5. Monetary instruments such as Travelers' Cheque
6. Foreign correspondent accounts
7. Trade finance (such as letters of credit)
8. Special use or concentration accounts
9. Lending activities, particularly loans secured by cash collateral and marketable securities
10. Non-deposit account services such as Non-deposit investment products and Insurance
11. Transactions undertaken for non-account holders (occasional customers)
12. Provision of safe custody and safety deposit boxes
13. Currency exchange transactions
14. Project financing of sensitive industries in high-risk jurisdictions
15. Trade finance services and transactions involving high-risk jurisdictions
16. Services offering anonymity or involving third parties
17. Services involving banknote and precious metal trading and delivery
18. Services offering cash, monetary or bearer instruments; cross-border transactions, etc.

IV. INDICATIVE LIST OF HIGH / MEDIUM RISK GEOGRAPHIES/ LOCATIONS/ COUNTRIES

Countries/Jurisdictions

1. Countries subject to sanctions, embargoes or similar measures in the United Nations Security Council Resolutions ("UNSCR").
2. Jurisdictions identified in FATF public statement as having substantial money laundering and terrorist financing (ML/FT) risks (www.fatf-gafi.org)
3. Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies (www.fatf-gafi.org)
4. Tax havens or countries that are known for highly secretive banking and corporate law practices
5. Countries identified by credible sources1 as lacking appropriate AML/CFT laws, regulations and other measures.
6. Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
7. Countries identified by credible sources as having significant levels of criminal activity.
8. Countries identified by the bank as high-risk because of its prior experiences, transaction history, or other factors (e.g. legal considerations, or allegations of official corruption).

Locations

1. Locations within the country known as high risk for terrorist incidents or terrorist financing activities (e.g. sensitive locations in Jammu and Kashmir, North east, Naxal affected districts)
2. Locations identified by credible sources as having significant levels of criminal, terrorist, terrorist financing activity.

3. Locations identified by the bank as high-risk because of its prior experiences, transaction history, or other factors.

ANNEXURE 13.5 – RED FLAG INDICATORS FOR SUSPICIOUS TRANSACTIONS BUILT INTO THE AML SOFTWARE OF THE BANK

a) System Based Alerts raised at the Branch Level

Source of alert	Red Flag Indicator
CV – Customer Verification	Wrong address, forged documents etc. provided by customer
LQ – Law Enforcement Agency Query	Customer investigated for TF offences/Blocking order received
MR – Media Reports	Adverse media reports about customer on TV/Newspaper etc.
EI – Employee Initiated	Customer has no explanation for source of funds, is secretive/nervous or attempted transaction by customer
PC – Public Complaint	Complaint received against customer by public-frauds committed
BA – Business Associates	Alert raised by agents/other institutions against customer

b) If the accounts with genuine transactions are being repeatedly hit by the alerts due to the threshold limits. All whitelisting of alerts to be documented with the reasons by the Branch Manager/Group Office.

c) Generation of Alerts at Branch Level – System Based –

Source of alert	Red Flag Indicator
WL – Watch List	Customer details matched with watch lists (e.g. UN list, Interpol list etc.)
TY – Typology	Common typologies/patterns of money laundering, terrorist financing (e.g. structuring of cash deposits/splitting of cash transactions, routing through multiple accounts)
TM – Transaction Monitoring	Transaction based alerts (unusually large transactions, sudden increase in volume, high value cash deposit/withdrawal)
RM – Risk Management System	Risk management system based alert (eg. high risk customer, country, location, source of funds, transaction type)

Parameters built into the Generation of Alerts at Branch Level based on –

WL – Watch List

(i) Match with UN List - UN List to be provided into the system to search and match
(ii) Match with UAPA List - UAPA List to be provided into the system to search and match
(iii) Match with TF List - TF List to be provided into the system to search and match.
(iv) Match with other criminal list - Any other criminal list to be provided into the system to search and match.
(v) Match with Geographies - As per list provided.

TM – Transaction Monitoring

(i) High value cash deposits in a day: Cash deposits aggregating to Rs.2 lakhs or more for individuals and Rs.10 lakhs or more for non-individuals in a day.

(ii) High value cash withdrawals in a day: Cash withdrawals aggregating to Rs.5 lakhs or more for individuals and Rs.10 lakhs or more for non-individuals in a day.

(iii) High value non-cash deposits in a day: Non-cash deposits greater than Rs.10 lakhs for individuals and Rs.25 lakhs for non-individuals in a day.

(iv) High value non-cash withdrawals in a day: Non-cash withdrawals greater than Rs.10 lakhs for individuals and Rs.25 lakhs for non-individuals in a day.

(v) High value cash deposits in a month: Cash deposits aggregating to greater than Rs.10 lakhs, Rs.8 lakhs and Rs.6 lakhs for individuals and Rs.50 lakhs, Rs.40 lakhs and Rs.30 lakhs for non-individuals in a month.

(vi) High value cash withdrawals in a month: Cash withdrawals aggregating to greater than Rs.10 lakhs, Rs.8 lakhs and Rs.6 lakhs for individuals and Rs.50 lakhs, Rs.40 lakhs and Rs.30 lakhs for non-individuals in a month.

(vii) High value non-cash deposits in a month: Non-Cash deposits aggregating to greater than Rs.40 lakhs, Rs.30 lakhs and Rs.20 lakhs for individuals and Rs.10 crores, Rs.5 crores and Rs.2 crores for non-individuals in a month.

(viii) High value non-cash withdrawals in a month: Non-Cash withdrawals aggregating to greater than Rs.40 lakhs, Rs.30 lakhs and Rs.20 lakhs for individuals and Rs.10 crores, Rs.5 crores and Rs.2 crores for non-individuals in a month.

(ix) Sudden high value transaction for the client: Value of a transaction more than Rs.5 lakhs for individuals and Rs.20 lakhs for non-individuals is more than 150% of the previous largest transaction for the client for last three months preceding the transaction.

(x) Sudden increase in value of transactions in a month for the client: Value of transactions is more than Rs.10 lakhs for individuals and Rs.50 lakhs for non-individuals and exceeds 150% of the monthly average of the account turnover (total value of debit and credit transactions in a month) for the preceding quarter.

(xi) Sudden increase in number of transactions in a month for the client: Monthly account activity (total number i.e. 25 of debit and credit transactions in a month) aggregating to more than Rs.10 lakhs for individuals and Rs.50 lakhs for non-individuals and exceeds the monthly average of account activity of the preceding quarter by 150%.

(xii) High value transactions in a new account: Transactions greater than Rs.2 lakhs for individuals and Rs.5 lakhs for non-individuals in newly opened account within 1 month of account opening.

(xiii) High activity in a new account: Number of transactions more than 15 for individuals and 40 for non-individuals in a newly opened account within 1 month of account opening.

(xiv) High value transactions in a dormant account: Transactions greater than Rs.2 lakhs for individuals and Rs.5 lakhs for non-individuals in a dormant account within 15 days of reactivation.

(xv) Sudden activity in a dormant account: Number of transactions more than 5 for individuals and 10 for non-individuals in a dormant account within 15 days of reactivation.

(xvi) High value cash transactions inconsistent with profile: Cash transactions greater than Rs.1 lakh by customer with low cash requirements such as Students, Housewife, Pensioners, Wages and Salary Person and Minor Accounts.

(xvii) High cash activity inconsistent with profile: Number of cash transactions more than 15 times in a month by a customer with low cash requirements such as Students, Housewife, Pensioners, Wages and Salary Person and Minor Accounts.

(xviii) Sudden increase in cash deposits of customers: Cash deposits aggregating to more than Rs.5 lakhs, Rs.3 lakhs and Rs.2 lakhs for individuals and Rs.10 lakhs, Rs.7 lakhs and Rs.5 lakhs for non-individuals in a month exceeds the monthly average of cash deposits in the preceding month.

(xix) Sudden increase in cash withdrawals of customers: Cash withdrawals aggregating to more than

Rs.5 lakhs, Rs.3 lakhs and Rs.2 lakhs for individuals and Rs.10 lakhs, Rs.7 lakhs and Rs.5 lakhs for non-individuals in a month exceeds the monthly average of cash withdrawals in the preceding month.

(xx) High value cash transactions in accounts without PAN: High value cash transactions above Rs.50,000/- in a month for accounts without PAN.

(xxi) High value non-cash transactions in accounts without PAN: High value non-cash transactions above Rs.2 lakhs for individuals and Rs.5 lakhs for non-individuals in a month for accounts without PAN.

(xxii) GST Refund Fraud: GST refund credits more than Rs.2 lakhs for individuals and Rs.5 lakhs for non-individuals and more than 125% of total account credits during 90 days.

(xxiii) Immediate transfer of funds and very low minimum balance maintained in account: Cash/Non-cash deposits in accounts greater than INR Rs.2 lakhs, Rs.3 lakhs and Rs.5 lakhs for individuals and Rs.20 lakhs, Rs.15 lakhs and Rs.10 lakhs for non-individuals followed by non-cash withdrawals of 75% or more within a day and low Account Balance less than Rs.10,000/- for individuals and Rs.25,000/- for non-individuals maintained.

TY – Typology

(i) Splitting of cash deposits just below Rs.10,00,000/- in single/multiple accounts in a month: Cash deposits in amounts ranging between Rs.2.00 lakhs for individuals and Rs.5.00 lakhs for non-individuals to maximum amount Rs.999,999.99 in single/multiple accounts of the customer greater than 5 times for individuals and 8 times for non-individuals in a month.

(ii) Splitting of cash deposits just below Rs.50,000/-: Cash deposits in amounts ranging between Rs.10,000/- for individuals and Rs.15,000/- for non-individuals to maximum amount of Rs.49,999.99 in single/multiple accounts of the customer greater than 10 times for individuals and 15 times for non-individuals in a month.

(iii) Repayment of loan in cash: Loan repayments in cash greater than 75% of total repayments in last 6 months with a minimum loan disbursement value of Rs.10 lakhs in non-individual accounts.

(iv) Repayment of loan in cash: Loan repayments in cash greater than Rs.5.00 lakhs in 1 month for non-individual accounts.

(v) Premature closure of large FDR through PO/DD: Premature closure of FDR for amounts greater than Rs.5.00 lakhs within 30 days and payment by PO/DD.

(vi) Frequent low cash withdrawals: Cash withdrawals in amounts ranging between Rs.10,000/- to Rs.50,000/- for individuals and Rs.25,000/- to Rs.1 lakh for non-individual in single or multiple accounts of the customer greater than 10 times for individuals and 20 times for non-individuals in 30 days.

(vii) Many to one fund transfer: Funds aggregating to Rs.5 lakhs, Rs.3 lakhs and Rs.2 lakhs for individuals and Rs.10 lakhs, Rs.7 lakhs and Rs.5 lakhs for non-individuals sent by more than 8 remitters for individuals and 15 remitters for non-individuals to one recipient in a month both for domestic and cross border transactions.

(viii) One to many fund transfer: Funds aggregating to Rs.5 lakhs, Rs.3 lakhs and Rs.2 lakhs for individuals and Rs.10 lakhs, Rs.7 lakhs and Rs.5 lakhs for non-individuals sent by one remitter to more than 8 recipients for individuals and 15 recipients for non-individuals in a month both for domestic and cross border transactions.

(ix) Routing of funds through multiple accounts: Transactions greater than Rs.2 lakhs for individuals and Rs.5 lakhs for non-individuals and between more than 5 accounts in the same bank aggregating to more than Rs.10 lakhs for individuals and Rs.25 lakhs for non-individuals on the same day.

(x) Repeated small value cash deposits followed by immediate cash withdrawals from different locations: Cash deposits in amounts ranging between Rs.50,000/- to Rs.5 lakhs for individuals and Rs.10 lakhs for non-individuals greater than 10 times in a day followed by immediate cash withdrawals of 75% or more of total cash deposits from different locations.

(xi) Repeated small value transfers from multiple parties followed by immediate cash/ non-cash withdrawals (through ATMs or other modes): Receipt of account to account transfer (RTGS/NEFT/IMPS/ transfer, etc.) from multiple parties in amounts ranging between Rs.50,000/- to Rs.5 lakhs for individuals and Rs.10 lakhs for non-individuals greater than 10 times in a day followed by immediate cash / non-cash withdrawals of 75% or more of such deposits.

RM – Risk Management System

(i) NPOs or charities receiving funds from India or abroad, and transferring the same to a number of domestic and foreign beneficiaries: Single large value deposit greater than Rs.10 lakhs, Rs.7 lakhs and Rs.5 lakhs for individuals and Rs.25 lakhs for non-individuals for NPOs or charities followed by debits/transfers to more than 5 beneficiaries for individuals and 10 beneficiaries for no-individuals within 30 days.

(ii) High value cash transactions in NPO: Cash transactions greater than Rs.10.00 lakhs for Savings account and Rs.25.00 lakhs for Current accounts in Trust/ NGO/NPO in 30 days.

(iii) High value cash transactions pertaining to accounts of real estate agents and dealers: Cash transactions (deposits and withdrawals) aggregating to greater than Rs.10 lakhs pertaining to accounts of real estate agents and dealers, in a month.

(iv) High value cash transactions by dealer in precious metal or stone: Cash transactions (deposits and withdrawals) aggregating to greater than Rs.10 lakhs by dealer in precious metal, precious stone and gems & jewellery, in a month.

(v) High value transactions in accounts opened and closed in a short duration: Account turnover (sum of credits and debits) of more than Rs.5 lakhs for individuals and Rs.10 lakhs for non-individuals in operative accounts closed within 15 days of opening the account.

(vi) High value transactions in new accounts followed by period of inactivity: Monthly Account turnover (sum of credits and debits) of more than Rs.5 lakhs, Rs.3 lakhs and Rs.2 lakhs for individuals and Rs.20 lakhs, Rs.15 lakhs and Rs.10 lakhs for non-individuals in newly opened operative account followed by period of inactivity in the account (no customer induced transactions for 3 months following the last transaction).

(vii) Unusually high activity in Current Account (CA): Number of transactions exceeding 75 transactions in CA (excluding public limited companies) in a month.

(viii) Multiple customers working together: Accounts opened by multiple unrelated customers linked by a common PAN, address, mobile number or email address.

(ix) Frequent Locker operations: Number of locker operations greater than 5 times in a month.

(x) Large repetitive debit card usage at the same merchant: Transactions greater than Rs.2 lakhs for individuals and Rs.5 lakhs for non-individuals exceeding 5 times in a day

(xi) High number of cheque leaves: Number of transactions through cheques more than 15 for individuals and 60 for non-individuals in a month.

(xii) Aggregate of all credits in a financial year in BSBDA Small accounts: Aggregate of all credits in BSBDA Small accounts exceeds Rs.99,999.99 for individuals in a financial year.

(xiii) Aggregate of all withdrawals and transfers in a month in BSBDA Small accounts: Aggregate of all withdrawals and transfers in BSBDA Small accounts exceeds Rs.9,999.99 in a month.

(xiv) Balance in BSBDA Small accounts: Balance in BSBDA small accounts exceeds Rs.49,999.99 on any given day.

d) Review of Alerts at Central Office and the suspicious transaction reported to Group Office for further enhanced due diligence (EDD) and verification of the transaction with the profile of the customer. On confirmation, the form prescribed in Annexure 13.6 to be duly filled in and duly signed by Branch Manager and Group Office and submitted to Compliance Department for further reporting.at FIU-India.

e) Based on the alerts and the investigation carried out by **Group Office, the case may be closed either as "Money Laundering investigated – False Positive" or "Money laundering report filed"** and all such alerts documented and reported to Principal Officer.

f) Preparation and Submission of Suspicious Transaction Report based on the above and submission to FIU-India within seven working days on being satisfied that the transaction is suspicious as per prescribed format of FIU-India.

ANNEXURE 13.6 - MONEY LAUNDERING/ SUSPICION REPORT FORMAT

This form should be used to document any suspicions of Money Laundering or Financial Crime. Once completed, the form should be sent immediately to the Principal / Compliance Officer.

Name:..... Branch/Department:.....

Reporter: Name **Designation:.....**
Branch / dept.

CUSTOMER:

Name:.....

Account Number:.....

Address:.....
.....
.....

SUSPICION REPORT: (*Record below details of the transaction or circumstances, reasons for your suspicion and the due diligence carried out. Continue on a separate sheet if necessary)*
Refer Annexure 13.7 Model Template for STR Reporting (GOS part) for recording the Grounds of Suspicion)

REPORTER'S SIGNATURE **BRANCH HEAD SIGNATURE**

DATE/TIME:.....

GROUP HEAD CONFIRMATION/OBSERVATION *(Include due-diligence undertaken)*

GROUP HEAD SIGNATURE

IMPORTANT NOTE TO THE REPORTER:
IT IS AN OFFENCE TO ADVISE THE CUSTOMER OR ANYONE OTHER THAN THE COMPLIANCE OFFICER/NOMINATED OFFICER OF YOUR SUSPICION AND THE FACT THAT YOU HAVE REPORTED IT

COMPLIANCE DEPT USE ONLY:

Date Received: **Time Received:** **Reference No.:**

Signature: **Date:**

Please return the completed form and any supporting documentation directly to the Principal / Compliance Officer, marked *"PRIVATE & CONFIDENTIAL"*

ANNEXURE 13.7 - MODEL TEMPLATE FOR STR REPORTING (GOS PART)

CUSTOMER KYC

1. **Full Name and Address of the account holder (including the company):** Full name and address as appearing in the OVD obtained for the latest KYC
2. **Date of Birth (for individual)/Date of incorporation for the company):** To be given in DDMMYYYY format
3. **PAN No**: 10 character long PAN Number must be given, if available with the Bank, else should be left Blank
4. **Passport No**: It is to be given if available with the Bank
5. **Other Identification documents**: Details of the other ID documents (Number and issuing office) may be given
6. **IEC Code**: To be given in all cases where the a/c holders deal in EXIM business
7. **GSTIN**: To be given in cases where account holder is trader or service provider
8. **Mobile number/Landline no**: To be given in full with STD code
9. **Other facilities availed:** Details may be given of other facilities like locker, FDs, loans etc.
10. **Risk Category**: Assigned by the bank should be given here
11. **Name of the authorised signing authorities**: Name of the concerned persons should be given
12. **KYC Compliance status:** Has KYC been done?
13. **Date of last KYC updation:** Should be given in DDMMYYYY format

CUSTOMER PROFILE

1. **Profile/Nature of business:** Should give the full information (e.g. Trading in food grains, Trading in Vegetable i.e. complete description instead of simply Trading
2. **Annual income as declared in KYC**: (Rs in lakhs)
3. **Annual Turnover of Business as declared in KYC:** (Rs in lakhs)
4. **Beneficial owner(s) as determined under Rule 9(3) of PMLA Rules**

ACCOUNT DETAILS

1. **Bank and Branch details**: Branch details are to be given (i.e. XXX Bank, MG Road, Bengaluru 560001)
2. **Bank account no**: Account no in full to be given
3. **Bank Account Type**: Saving/Current/Loan etc.
4. **Bank A/c opened on**: Should be given in DDMMYYYY
5. **Bank Account Status**: whether active or dormant or closed

TRANSACTION SUMMARY

1. **Quantum of transactions for the current year**: Debit side Rs. XX lakhs (in cash Rs. XX lakhs) and Credit side Rs. XX lakhs (in cash Rs. XX lakhs) (Restrict to current year only)
2. **Quantum of transactions for previous years**: For the last 3 years Debit side Rs. XX lakhs (in cash Rs. XX lakhs) and Credit side Rs. XX lakhs (in cash Rs. XX lakhs) individual year wise
3. **Balance in account on date of filing STR**

HISTORY

1. **Details of earlier STR filed on the account or account holders/related persons**: Batch ID, Sr. No. reported a/c number and name of the a/c holder may also be given in respect of the previously filed STRs, if any

REASONS FOR SUSPICION

1. **Reactive STR**: If the STR is filed on the basis of an inquiry from an LEA (including alerts issued from FIU-IND office), full details of the query letter (letter no and date), issuing office and signing authority may be stated. It may also be added if the information sought for has been given.
2. **Adverse media report**: Link details to the media report may be given. In such cases, the Bank should also do the Enhanced Due Diligence and findings thereof should be included in GoS
3. **Grounds of Suspicion:** Bank should explain clearly the reason why a particular transaction of set of transactions were found suspicious, The GoS may also include transaction pattern, if the Bank can find one. The Bank should also state specifically as to what appears to be the suspicion for raising the STR-Tax evasion, Trade Based Money Laundering (TBML), Terror Financing (TF), Laundering of money earned from criminal activities, anti-national activities, corruption, frauds, forgery, perfect match with watchlists etc.
4. **Details of investigation**: The Bank must give complete details of the suspected transaction(s). While giving this information, details of creditors/debtors (name, bank and a/c number) may also be given, if available, with the Bank.

ANNEXURE 13.8 - BENEFICIAL OWNER DECLARATION

On the Letter Head of the Company/Firm/Trust.

To:

The Manager _____branch

Sub:-Declaration regarding Beneficial Ownership

I/We are the authorized signatory(ies) of _____
Company/ Partnership firm /Trust / Others. Following are the details of the company/ Partnership firm/ Trust which wants to open an account with your Bank/ already having account no. at your branch.

Name of the account: _____**Core Banking A/c Number:** _____

Names of all partners / trustees / Directors of Private Ltd Company along with % of sharing or ownership control over the business.

Sr. No	Name of the partners /trustees/Directors	% of sharing or ownership control over the business	PAN	Contact No.	Address

I/We hereby state and confirm that what is stated above is true and correct information.

I/We hereby declare that the I/we am/are the only persons who own/s and controls the affairs of my /our business and thereby declare myself/ ourselves as Beneficial Owner

I/we agree to indemnify and keep indemnified at all times from and against all costs, charges, damages .penalties (including reasonable attorney fees) suffered and /or incurred by the Bank any act done or omitted to be done on the above declaration.

Signature(s) of the Authorized Signatories along with Rubber stamp.

**** **Instructions**: These fields are mandatory along with the documentary proof in case of the 'Beneficial Owners' defined as follows.

Partnership Firm: Ownership of /entitlement to more than 15 % of capital or profits

Trust: 15% or more interest in the trust and any other natural persons exercising ultimate effective control over the trust through a chain of control or ownership

Company (Other than company listed on a stock exchange, or is a majority -owned subsidiary of such a company): Ownership of /entitlement to more than 25% of shares or capital or profits

Unincorporated association or body of individuals: Ownership of / entitlement to more than 15 percent of property or capital or profits

Where no natural person can be identified, senior most official to be identified.

ANNEXURE 13.9 - UNLAWFUL ACTIVITIES (PREVENTION) ACT, 1967 (UAPA)

***Section 17** of UAPA* reads as under:
"Whoever, in India or in a foreign country , directly or indirectly, raises or collects funds or provides funds to any person or persons or attempts to provide funds to any person or persons, knowing that such funds are likely to be used by such persons to commit a terrorist act, notwithstanding whether such funds were actually used or not for commission of such act, shall be punishable with imprisonment for a term which shall not be less than five years but which may extend to imprisonment for life, and shall also be liable to fine".

***Section 40** of UAPA* criminalises raising of funds for terrorist organisations listed in the Schedule to UAPA and reads as under:
"A person commits the offence of raising fund for a terrorist organisation, who, with intention to further the activity of a terrorist organisation, (a) invites another person to provide money or other property, and intends that it should be used, or has reasonable cause to suspect that it might be used, for the purposes of terrorism; or (b) receives money or other property and intends that it should be used, or has reasonable cause to suspect that it might be used for the purposes of terrorism; or (c) provides money or other property , and knows, or has reasonable cause to suspect , that it would or might be used for the purposes of terrorism. A person who commits the offence of raising fund for a terrorist organisation under sub-section (1) shall be punishable with imprisonment for a term not exceeding fourteen years, or with fine, or with both".

FREEZING OF ASSETS under Section 51A of Unlawful Activities (Prevention) Act, 1967 and Implementation of requests received from Foreign Countries under U.N. Security Council Resolution 1373 of 2001

In terms of Section 51A, Unlawful Activities (Prevention) Act, 1967, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism and prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

On receipt of the list of individuals and entities subject to UN sanctions from RBI, Bank shall ensure expeditious and effective implementation of the procedure prescribed under Section 51A of UAPA in regard to freezing/unfreezing of financial assets of the designated individuals/entities enlisted in the UNSCRs and especially, in regard to funds, financial assets or economic resources or related services held in the form of bank accounts.

In terms of Para 4 of the Order, in regard to funds, financial assets or economic resources or related services held in the form of bank accounts, the RBI would forward the designated lists to the banks requiring them to:

a) Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of bank accounts with them.

b) In case, the particulars of any of the customers match with the particulars of designated individuals/entities, the Bank shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, held by such customer on their books to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail:

c) Bank shall also send by post a copy of the communication mentioned in (b) above to the UAPA nodal officer of RBI, Chief General Manager, Department of Banking Operations and Development, Anti Money Laundering Division, World Trade Centre, Centre-1, 4th Floor, Cuffe Parade, Colaba, Mumbai –400005 and also by fax at No.022-22185792. The particulars apart from being sent by post/fax should necessarily be conveyed on e-mail:
d) Bank shall also send a copy of the communication mentioned in (b) above to the UAPA nodal officer of the state/UT where the account is held as the case may be and to FIU-India.
e) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the Bank would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on email:
f) Bank shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (b) above, carried through or attempted, as per the prescribed format.

I. Freezing of Financial Assets
On receipt of the particulars IS-I Division of Ministry of Home Affairs (MHA) would cause a verification to be conducted by the State Police and / or the Central Agencies so as to ensure that the individuals / entities identified by the banks are the ones listed as designated individuals / entities and the funds, financial assets or economic resources or related services, reported by banks are held by the designated individuals / entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars. In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals / entities, an order to freeze these assets under section 51A of the UAPA would be issued by The Joint Secretary (IS-I), MHA within 24 hours of such verification and conveyed electronically to the bank branch concerned under intimation to Reserve Bank of India and FIU-IND. The order shall take place without prior notice to the designated individuals / entities.

II. Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals / entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person.
Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned / held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the Bank.
The Bank shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact details given within two working days with a copy to the Principal Officer.
The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual / entity and if he is satisfied, he shall pass an order, within **five** working days, unfreezing the funds, financial assets or economic resources or related services, owned / held by such applicant under intimation to the concerned bank. However, if it is not possible for any reason to pass an order unfreezing the assets within **five** working days, the nodal officer of IS-I Division shall inform the applicant.

III. Communication of Orders under the Section 51A of Unlawful Activities (Prevention) Act
All Orders under Section 51A of Unlawful Activities (Prevention) Act, relating to funds, financial assets or economic resources or related services, will be communicated to the branches on receipt of communication from RBI and the same will be uploaded on the system.