JANATA SAHAKARI BANK LTD., PUNE

(MULTI-STATE SCHEDULED BANK)

HEAD OFFICE – 1444, SHUKRAWAR PETH, THORALE BAJIRAO ROAD, PUNE – 411002

KYC – AML – CFT

AMLCELL

KYC-AML OWNERSHIP IS OUR COMMITMENT

PREFACE

The policy is prepared with respect to the requirements of RBI's Master Direction on KYC, 2016 as updated up to 04.05.2023, Risk Based Approach to KYC-AML, 174 Red Flag Indicators and also in consideration to and instructions being received in the course of statutory audit, RBI Inspection, amendments made in KYC AML Guidelines, various outreach meetings conducted jointly by FIU-IND and RBI, and various workshops conducted by RBI. Also, the supplementary policy for the year 2022-23 is included in this policy. The points in the sanctioned note by Hon. CEO regarding 'Changes to be made in existing systems and procedures' are also considered in this policy.

As instructed in various RBI workshops, policies of different banks were also referred in formulating this policy.

Policy layout is designed as per instructions of Planning Department.

Regards,

Mr. Deepak Kelkar
Deputy General Manager
AML Cell

Mr. Dhananjay Sahasrabudhe
General Manager
AML Cell

INDEX

Sr. No	Contents			Page
1.	INTRODUCTION			4
2.	OBJECTIVES / PURPOSE OF THE POLICY			5
3.	SCOPE OF THE POLICY			5
4.	ABBREVIATIONS			6
5.	POLICY			7
	5.1	ORGANIZATION STRUCTURE		8
	5.2	DEFINITIONS		11
	5.3	KYC AML CFT POLICY GUIDELINES		
		5.3.1	CUSTOMER ACCEPTANCE POLICY	21
		5.3.2	CUSTOMER IDENTIFICATION POLICY	25
		5.3.3	KYC / CKYC / RE-KYC COMPLIANCE	32
		5.3.4	LEGAL ENTITY / BENEFICIAL OWNER / LEGAL ENTITY IDENTIFIER	37
		5.3.5	DUE DILIGENCE	40
		5.3.6	RISK MANAGEMENT	
			5.3.6.1 – RISK IDENTIFICATION, MEASUREMENT, MITIGATION AND REVIEW MECHANISM. 5.3.6.2 – RISK CATEGORIZATION OF THE CUSTOMER. 5.3.6.3 – RISK ASSESSMENT OF THE BANK.	50 51 54
		5.3.7	REPORTING REQUIREMENT UNDER FATCA / CRS	57
		5.3.8	OBLIGATIONS UNDER PMLA, 2020	57
			5.3.8.1 – MAINTENANCE OF RECORD OF TRANSACTION 5.3.8.2 – INFORMATION TO BE PRESERVED 5.3.8.3 – MAINTENANCE AND PRESERVATION OF RECORD 5.3.8.4 – REPORTING TO FIU-INDIA 5.3.8.5 – MONITORING OF TRANSACTIONS	59 60 60 62 65
		5.3.9	TRAINING	69
		5.3.10	FRAUDS- CLASSIFICATION AND REPORTING	70
		5.3.11	RISK BASED APPROACH TO KYC-AML QUARTERLY SUPERVISION DATA & YEARLY DOCUMENTS	79
		5.3.12	PROVISIONS UNDER UAPA, 1967	81
		5.3.13	PROVISIONS UNDER WMD ACT, 2005	101
		5.3.14	GENERAL GUIDELINES	104
6.	ANNEXURES			117

1. INTRODUCTION

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), banks were advised by RBI to ensure that a proper policy framework on 'Know Your Customer and Anti-Money Laundering' measures is formulated and put in place with the approval of the Board. Accordingly, bank's policy on 'KNOW YOUR CUSTOMER (KYC)' norms, 'ANTI MONEY LAUNDERING (AML)' and Combating Financing Terrorism (CFT) measures, is approved and adopted by the Board of Directors.

Know Your Customer is the process of verifying the identity of customer. The objective of KYC/AML/CFT guidelines is to prevent banks/FIs from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable banks/FIs to know/understand their customers and their financial dealings better and manage their risks prudently.

RBI has issued the guidelines under Section 35 A of the Banking Regulation Act, 1949 and the Banking regulation Act (AACS), 1949, read with section 56 of the ibid and Rule 9(14) of Prevention of Money Laundering (Maintenance of records) Rules 2005 the Reserve Bank of India being satisfied that it is necessary and expedient in the public interest to do so, here by issues the direction here in after specified 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 and any contravention thereof or non-compliance may attract penalties under Banking Regulation Act.

This policy document is approved by the Hon. Board and is prepared in accordance with the requirements of RBI's Master Direction on KYC, 2016 as updated up to 04.05.2023, Risk Based Approach to KYC-AML, 174 Red Flag Indicators and also in consideration to and instructions being received in the course of statutory audit, RBI Inspection, amendments made in KYC AML Guidelines, various outreach meetings conducted jointly by FIU-IND and RBI, and various workshops conducted by RBI. Also, the supplementary policy for the year 2022-23 is included in this policy. The points in the sanctioned note by Hon. CEO regarding 'Changes to be made in existing systems and procedures' are also considered in this policy.

Whenever any of the directions / circulars / guidelines are updated by the regulatory authorities, the bank will implement the same in the policy with prior approval of the Hon BoD with retrospective effect, wherever applicable.

The newly formulated Standard Operating Procedures (SOPs) and formats for Re-KYC declaration, CKYCR template, etc. will form a part of this policy and will help in actual execution of the policy.

2. OBJECTIVES / PURPOSE OF THE POLICY

A. To lay down policy framework for abiding by the Know Your Customer (KYC) norms and Anti Money Laundering (AML) Measure as set out by Reserve Bank of India, based on the recommendations of the Financial Action Task Force (FATF) and the paper issued on Customer Due Diligence (CDD) for banks issued by the Basel Committee on Banking Supervision.
B. To prevent the Bank from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.
C. To enable the Bank to know / understand its customers and their financial dealings better, which In turn shall help it to manage its risks prudently.
D. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws / laid down procedures and regulatory guidelines.
E. To ensure that the policy is meticulously followed by the staff and are well versed with all its aspects.
F. To ensure compliance of PML Act/Rules by adopting best practices and taking into account FATF standards / guidelines as set out by RBI for managing risks better.

3. SCOPE OF THE POLICY

A. This policy shall be applicable across all offices of the bank and its branches.
B. The policy shall be applicable to all the products and services offered by the bank & all the business segments of the Bank.
C. The policy shall be read in conjunction with all other policies of the bank and related procedures, or operational guidelines issued from time to time.
D. The contents of the policy shall always be read in tandem / auto-corrected with the changes / modifications / which may be advised by RBI and / or by any regulators and /or by Bank from time to time.

4. ABBREVIATIONS

KYC – Know Your Customer	RBA – Risk Based Approach
AML – Anti Money Laundering	SOP – Standard Operating Procedure
CFT – Combating Financing of Terrorism	CKYCR – Central KYC Records Registry
RBI – Reserve Bank of India	KIN – KYC Identification Number
FIU-IND – Financial Intelligence Unit – INDIA	UCIC – unique Customer Identification Code
CDD – Customer Due Diligence	FIR – First Information Report
EDD – Enhanced Due Diligence	CTCR – Counter Terrorism Counter Radicalisation
FATF – Financial Action Task Force	VRV – Count of Vigilance Scenario Violation
UAPA – Unlawful Activities (Prevention) Act	SDN – Specified Designated Nationals
PMLA – Prevention of Money Laundering Act	NGO – Non-Government Organisations
STR – Suspicious Transaction Report	FMR – Fraud Monitoring Report
CCR – Counterfeit Currency Report	FUA – FMR Update Application
NTR – Non-profit making organisation Transaction Report	ODD – On-going Due Diligence
CTR – Cash Transaction report	SDD – Simplified Due Diligence
RFI – Red Flag Indicators	DD/PO–Designated Director/Principal Officer
CCO – Chief Compliance Officer	CRO – Chief Risk Officer
BO – Beneficial Owner	LE – Legal Entity
FEMA – Foreign Exchange Management Act	NRI – Non Resident Indian
OVD – Officially Valid Documents	CIP – Customer Identification Policy
CAP – Customer Acceptance Policy	V-CIP – Video based Customer Identification Policy
BOI – Body Of Individuals	AOI – Association of Persons
PEP – Politically Exposed Persons	UN- OFAC – United Nations – Office of Foreign Assets Control
FATCA – Foreign Account Tax Compliance Act	CRS – Common Reporting Standards
ML / TF – Money Laundering / Terrorist Financing	PAN – Permanent Account Number
OTP – One Time Password	BC – Business Correspondent
UIDAI – Unique Identification Authority of India	MCA – Ministry of Corporate Affairs
MHA – Ministry of Home Affairs	CIN – Company Identification Number
DIN – Director Identification Number	CERSAI - Central Registry of Securitisation Asset Reconstruction and Security Interest of India
SHG – Self Help Group	FPI – Foreign Portfolio Investors
IBA – Indian Bank Association	GoS – Ground of Suspicion.

5. POLICY

5.1. Organisational Structure

The Board of Directors shall be responsible for the following:

A. To decide the policies of the bank with regards to KYC-AML measures and its compliance.

B. To advise / guide the field functionaries.

- **Audit Inspection Committee**

A committee of Hon. Board of Directors was constituted according to the newly elected Hon. Board of Directors for Audit Inspection purpose as per resolution no 182/1/11 dated 25/08/2022 comprising of the following members as under:

Sr. No.	Hon. Member Name	Designation
1.	CA Mr. K. V. Gandhi	Chairman
2.	Mr. M. M. Abhyankar	Member
3.	CA Mr. M. R. Mate	Member
4.	Mr. M. S. Phatak	Member
5.	Mr. S. D. Paraspatki	Member

- **High Value Fraud Monitoring Committee**

A committee of Hon. Board of Directors was constituted according to the newly elected Hon. Board of Directors for monitoring high value frauds as per resolution no 168/1/7 dated 30/07/2022 comprising of the following members as under:

Sr. No.	Hon. Member Name	Designation
1.	Mr. R B Hejib	Chairman
2.	Adv. Mrs. A V Petkar	Member
3.	CA Mr. M. R. Mate	Member
4.	Mr. P. T. Paranjape	Member
5.	Mr. A. Y. Ghaisas	Member
6.	Mr. M. S. Phatak	Member

➢ **Formation of KYC-AML Executive Committee**

A committee of Senior Executives namely KYC-AML Executive Committee was constituted for discussing and resolving KYC AML measures as per new organizational chart dated 22/05/2023 sanctioned in the capacity of Hon. Chief Executive Officer note no. 278 dated 08/03/2023 namely KYC-AML Executive Committee as under:

Sr. No.	Designation	Department	Committee post/designation
1.	General Manager	Audit Inspection (Principal Officer)	Chairman
2.	General Manager	IT	Member
3.	General Manager	Loan Department	Member
4.	General Manager	Legal and Recovery	Member
5.	Dy. General Manager	Administration	Member
6.	Dy. General Manager	KYC-AML-CBOC	Member
7.	Dy. General Manager	CPC Pune	Member
8.	Asst. General Manager	IT	Member
9.	Chief Compliance Officer	Compliance	Standing member
10.	Chief Risk Officer	Risk management	Standing member
11.	Chief Officer	KYC-AML	Secretary

The minimum quorum of the Executive Committee will be 4 members out of which President and Secretary are mandatory. The meeting will be held as and when required but atleast once every quarter.

The Executive committee shall be responsible for and will authorize the following:

- For smooth implementation of the banks KYC / AML Policy
- To decide the set of rules / parameters / values for transaction monitoring for STR detection.
- To decide roles and responsibilities of the functionaries in AML cell.
- To issue operational guidelines for AML cell.
- To appraise the Top Management of the status of PMLA compliance of the bank.

The Executive Committee shall also be the competent authority to

- frame rules for generation of alerts in the AML application for all those transactions which fulfill the criteria mentioned in the KYC AML Procedures for generation of alerts.
- modify/amend the existing rules for generation of alerts in the AML application.
- decide the values of the parameters required to be set for the implementation of rules for generation of alerts.
- decide whether a transaction shall be reported as STR.

- ratify the decisions made by the KYC-AML Sub Committee.

➢ **Formation of KYC-AML Sub Committee**

A committee named KYC-AML Sub Committee is constituted vide Sanction note no. 278 dated 08/03/2023 in the capacity of Hon. CEO with a view to have an in-depth and comprehensive discussion on short intervals. The said Committee will play a supportive role in the decision-making process of the KYC-AML Executive Committee. The members of the committee comprise of the following:-

Sr. No.	Designation	Department	Committee post/ designation
1.	Dy. General Manager	KYC-AML-CBOC	Chairman
2.	Chief Compliance Officer	Compliance	Member
3.	Chief Officer	IT	Member
4.	Chief Officer	KYC-AML-CBOC	Member

All the four members will be the required quorum for the meeting of the KYC-AML Sub Committee. The meeting is ought to be held as and when required but at least once in a calendar month. The formalities and protocols like agenda, minutes, ATR will not be mandatory for the Sub-Committee meeting although the reporting of all meetings held should be made to Hon. CEO through monthly review note of the department.

The committee shall be responsible / authorized for the following:

- Necessary decisions for smooth implementation of the banks KYC / AML Policy
- Determine the action to implement the decision taken by the main committee.
- Follow up to the concerned branches/ department for implementation.

➢ **Formation of Fraud Monitoring Committee-**

A committee named Fraud Monitoring Committee is constituted vide Sanction note no. 277 dated 08/03/2023 in the capacity of Hon. CEO for monitoring frauds and reporting them to RBI and it's concerned authorities. The said Committee comprises of the following members: -

Sr. No.	Designation	Department	Committee post/ designation
1.	Chief Compliance Officer	Compliance	Chairman
2.	Dy. General Manager	KYC-AML-CBOC	Member
3.	Asst. General Manager	Legal Recovery	Member
4.	Asst. General Manager	Accounts	Member
5.	Chief Officer	Administration	Member

6.	Senior Officer	NPA	Member
7.	Senior Officer	KYC-AML	Member
8.	Chief Officer	KYC-AML	Secretary

- **STR Committee**

A STR Committee is formed exclusively for the purpose of finalizing and reporting of STRs to FIU-IND, the working of which will start from 01.04.2023. The committee will comprise of the following:-

Sr. No.	Designation	Department	Committee post/ designation
1.	General Manager / Principal Officer	AML Cell– President	President
2.	Dy. General Manager	AML Cell	Member
3.	Chief Officer	AML Cell	Member
4.	Senior Officer	AML Cell	Secretary
5.	Senior Officer	AML Cell	Member
6.	Senior Officer	AML Cell	Member

The quorum of the meeting will be 3 members with President and Secretary being mandatory attendees. The meeting of the committee will be held as and when required. This committee is formulated for reducing the turnaround time (TAT) from alert generation to alert reporting to FIU-IND.

- **Appointment of Principal Officer**

A Senior Management Officer of the Bank shall be designated as Principal Officer of the Bank and he /she shall be located at the head / corporate office of the Bank and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. Principal Officer shall maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism. The Principal Officer shall act independently and report directly to the senior management or to the Board of Directors.

Appointment of Principal Officer will be in accordance with the resolution approved by the Hon. Board of Directors. Currently, General Manager – KYC AML Cell will act as Principal Officer and any change would require approval from the Hon. Board of Directors. New appointment, if any, should be conveyed to FIU-IND and RBI accordingly.

- **Role and Responsibility of Principal Officer**

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

The Principal Officer shall also be responsible for timely submission of CTR, STR and reporting of counterfeit notes (CCR) and all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency (NTR) to FIU-IND.

As per PML Rules, section 8, the Principal Officer should report to the Director all the submission (CTR, NTR and CCR) made to regulatory authorities every month within the prescribed timelines. Also, all suspicious transactions (STR) reported to FIU-IND should be conveyed to the Director within the prescribed timelines of being satisfied that the transactions are suspicious.

- **Designated Director**

Bank should nominate a Director on our Boards as "Designated Director" to ensure overall compliance with the obligations imposed under the Prevention of Money Laundering (Amendment) Act, 2012. As per RBI Circular No DCBR. CO. BPD. (PCB). No 1/14.01.062/2014-15 dated 05/11/2014, the bank may also appoint Senior Official from Management of the bank as a “Designated Director”.

The name, designation and address of the Designated Director shall be communicated to the FIU-IND and RBI. In no case, the Principal Officer shall be nominated as the 'Designated Director'.

Appointment of Designated Director will be in accordance with the resolution approved by the Hon. Board of Directors. New appointment, if any, should be conveyed to FIU-IND and RBI accordingly.

- **Appointment of Nodal Officer**

For overall compliance and reporting of RBA to KYC AML Quarterly (38) Supervision Data templates and 17 Yearly Standard Documents, as per RBI circular dated 08.04.2021, bank should mandatorily appoint a Nodal Officer as one point contact regarding the subject. Accordingly, Hon. CEO appointed Principal Officer / General Manager – KYC AML Cell as the Nodal Officer by approved note dated 27.06.2021.

- **Access to data / information**

With a view to enable the Designated Director / Principal Officer / Nodal Officer to discharge their responsibilities effectively, they and other appropriate staff shall have timely access to required data and other relevant information.

5.2. **<u>Definitions</u>** –

(A) In accordance with the sanction note dated 07/06/2021 in the capacity of Hon. CEO, in order to make the classification of total customers in the bank clear and uniform, the classification and definition of customers is as follows:-

i) Last customer number- Customer number allotted to last customer opened on a particular day.

ii) Block customers- These customer numbers were never allotted to any customer/ account holder, but it was allotted to various branches at the time of data migration of branches from various vendors to one vendor.

iii) Weed out customers- These customer numbers were weeded out/ wiped out from our system because there was no live account under these customers.

iv) In-Operative customers- No account can be opened under these customers and cannot operate the existing accounts which were opened under these customers.

v) Operative Customers- Can open new account under these customers and can operate existing accounts, existing under these customers.

Henceforth, the data of only operative customers should be reported to all our regulatory authorities i.e. RBI, FIU-INDIA etc. and to our Hon. ACB, Hon. BOD.

(B) Terms bearing meaning assigned in terms of Prevention of Money - Laundering Act, 2002 and the Prevention of Money - Laundering (Maintenance of Records) Rules, 2005:

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

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

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

iv. Beneficial Owner (BO)

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

Explanation- For the purpose of this sub-clause -

- "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company.
- "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 customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.

c. Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

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

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

e. Exemption from identification of BO:

The exemption from BO identification has been aligned with that provided in the PML Rules, 2005, such that where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or

(ii) is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or

(iii) is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such an entity.

v. "Certified Copy" - Obtaining a certified copy by the RE 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 authorised officer of the RE as per the provisions contained in the Act.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016{FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, may be obtained:

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

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

vii. "Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include:

a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,

b. the Managing Partner, if the RE is a partnership firm,

c. the Proprietor, if the RE is a proprietorship concern,

d. the Managing Trustee, if the RE is a trust,

e. a person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and

f. a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks.

Explanation - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.

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'

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

ix. "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).

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

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

xii. "Non-profit organizations" (NPO) - Non-profit organization means any entity or organization, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961)- By the drawing of Section 2(15) of the Income-tax Act, it defines the charitable purpose of the Act, which comprises relief to the poor, education, medical relief, and the improvement of any other object of general public utility of the Non-Profit Organization. Given that, charitable purposes under section 2(15) can get categorized under the following heads, that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013),

It includes the following:-

1. A trust established under the Indian Trust Act, 1882 for private trusts and under Bombay Public Trusts Act, 1950 for public trusts.
2. A society registered under Societies Registration Act, 1860
3. A Section 8 company registered under Companies Act, 2013
4. Trust registered as NGO
5. Society registered as NGO
6. Company registered as NGO

In Maharashtra and Gujarat, all societies must also simultaneously be registered as trusts under the Bombay Public Trusts Act, 1950

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

Provided that,

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

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

- utility bill which is not more than two months old of any service provider (electricity, telephone, post - paid mobile phone, piped gas, water bill);
- Property or Municipal tax receipt;
- 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 from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed

companies and leave and licence agreements with such employers allotting official accommodation;

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

d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India 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.

e. Provided that where 'simplified measures' are applied for verifying the identity of the clients the following documents shall be deemed to be OVD:

- identity card with applicant's Photograph issued by Central/ State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
- Letter issued by a gazetted officer, with a duly attested photograph of the person.

Provided further that where 'simplified measures' are applied for verifying for the limited purpose of proof of address the following additional documents are deemed to be OVDs:

- Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
- Property or Municipal Tax receipt;
- Bank account or Post Office savings bank account statement;
- 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 from employer issued by State or Central Government departments, statutory or regulatory bodies, and public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and
- Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India.

** Statutory Rules and Notifications as notified by UIDAI RBI Master Directions and PMLA Act

As per Notification issued by UIDAI and read with Aadhaar Regulation Act 2016, Chapter II, detailing restrictions on sharing of Identity Information and point No. 8 of the same Act which details the responsibility of any agency or entity with respect to Aadhaar Number as follow's-

(A) An individual, agency or entity which collects Aadhaar number or any document containing the Aadhaar number, shall:

(i)collect, store and use the Aadhaar number for a lawful purpose;

(ii)inform the Aadhaar number holder the following details:

(a)the purpose for which the information is collected;

(b)whether submission of Aadhaar number or proof of Aadhaar for such purpose is mandatory or voluntary, and if mandatory, the legal provision mandating it;

(c) Alternatives to submission of Aadhaar number or the document containing Aadhaar number, if any;
(iii) obtain consent of the Aadhaar number holder to the collection, storage and use of his
Aadhaar number for the specified purposes.
(B) Such individual, agency or entity shall not use the Aadhaar number for any purpose other than those specified to the Aadhaar number holder at the time of obtaining his consent.
(C) Such individual, agency or entity shall not share the Aadhaar number with any person
without the consent of the Aadhaar number holder. Also,
(D) The Aadhaar number of an individual shall not be published, displayed or posted publicly by any person or entity or agency.
(E) Any individual, entity or agency, which is in possession of Aadhaar number(s) of Aadhaar number holders, shall ensure security and confidentiality of the Aadhaar numbers and of any record or database containing the Aadhaar numbers.
(F) Without prejudice to sub-regulations (1) and (2), no entity, which is in possession of the Aadhaar number of an Aadhaar number holder, shall make public any database or record containing the Aadhaar numbers of individuals, unless the Aadhaar numbers have
been reacted or blacked out through appropriate means, both in print and electronic form. (Redacting or blacking out of Aadhaar number both in print and electronic form, before or after CKYC registration should be confirmed with CBOC Department.)
(G) No entity, including a requesting entity, shall require an individual to transmit his Aadhaar number over the Internet unless such transmission is secure and the Aadhaar number is transmitted in encrypted form except where transmission is required for correction of errors or redressal of grievances.
(H) No entity, shall retain Aadhaar numbers or any document or database containing Aadhaar numbers for longer than is necessary for the purpose specified to the Aadhaar number holder at the time of obtaining consent.

Simplified Measures for Proof of Identity: If an individual customer does not have any of the OVDs (as mentioned at paragraph above) as proof of identity, then banks/FIs are allowed to adopt 'Simplified Measures' in respect of 'Low risk' customers, taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved. Accordingly, in respect of low risk category customers, where simplified measures are applied, it would be sufficient to obtain a certified copy of any one of the documents referred to at proviso to paragraph above, which shall be deemed as an OVD for the purpose of proof of identity.

Simplified Measures for Proof of Address: The additional documents mentioned above shall be deemed to be OVDs under 'simplified measure' for the 'low risk' customers for the limited purpose of proof of address where customers are unable to produce any OVD for the same.

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

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

a. an individual,

b. a Hindu undivided family,

c. a company,

d. a firm,

e. an association of persons or a body of individuals, whether incorporated or not,

f. every artificial juridical person, not falling within any one of the above persons (a to e), and

g. any agency, office or branch owned or controlled by any of the above persons (a to f).

xvi. "Principal Officer" means an officer nominated by the RE, responsible for furnishing information as per rule 8 of the Rules. The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. The name, designation and address of the Principal Officer shall be communicated to the FIU-IND

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

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or

b. appears to be made in circumstances of unusual or unjustified complexity; or

c. appears to not have economic rationale or bona-fide purpose; or

d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

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

xviii. A 'Small Account' means a savings account which is opened in terms of sub-rule (5) of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are specified in Section 23.

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

a. opening of an account;

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

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

d. entering into any fiduciary relationship;

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

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

xx. "Video based Customer Identification Process (V-CIP)": an alternate method of customer identification with facial recognition and customer due diligence by an authorized official of the RE 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 Master Direction.

xxi. RBA to KYC AML Supervision Data means submission of KYC AML information in 38 quarterly templates and 17 yearly standard documents as specified in circular issued by RBI dated 08.04.2021.

xxii. Red Flag Indicators means newly introduced 174 alerts (rules) for effective detection and reporting of suspicious transactions divided in to 94 online alerts and 80 offline alerts as specified in FIU-IND circular dated 28.09.2020.

(B) Terms bearing meaning assigned in this Directions, unless the context otherwise requires, 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. "Customer" means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
iii. "Walk-in Customer" means a person who does not have an account-based relationship with the RE, but undertakes transactions with the RE.
iv. "Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner.
v. "Customer identification" means undertaking the process of CDD.
vi. "FATCA" means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.
vii. "IGA" means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.
viii. "KYC Templates" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
ix. "Non-face-to-face customers" means customers who open accounts without visiting the branch/offices of the REs or meeting the officials of REs.
x. "On-going Due Diligence" means regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.
xi. "Periodic Updation" means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.
xii. "Politically Exposed Person"- Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g. Heads of States or

of Governments, senior politicians, senior government / judicial / military officers, senior executives of State owned corporations, important political party officials, etc. Bank should gather sufficient information on any person / customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Bank should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for PEP will be taken by Branch Managers only. Bank will also subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, banks should obtain senior management approval to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

Even if one of the ultimate beneficial owner (UBO) of a legal entity customer is a PEP, then such legal entity customer should also be considered as a PEP customer as per our bank's policy.

xiii. "Regulated Entities" (REs) means

a. all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks'

b. All India Financial Institutions (AIFIs)

c. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs).

d. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)

e. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulate d by the Regulator.

xiv. "Shell Bank" means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

xv. "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.

xvi. "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.

xvii. Aadhaar Number: The Aadhaar Act means an identification number issued to an Individuals by Unique Identification Authority of India (UIDAI) on receipt of the demographic information and biometric information as per the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. In terms of the Aadhaar Act, every resident is eligible to obtain an Aadhaar number. Aadhaar is the document for identity and address.

xviii. Biometric information : Biometric information as defined in the Section 2(g) of the Aadhaar Act, means photograph, finger print, Iris scan, or such other biological attributes of an individual as may be specified by Aadhaar (authentication) regulations;
xix. Central Identities Data Repository ; CIDR means a centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto
xx. 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.
xxi. Demographic information : As per Aadhaar Act, information relating to the name, date of birth, address and other relevant information of an individual, as may be specified by regulations for the purpose of issuing an Aadhaar number, but shall not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history.
xxii. Enrolment number: Enrolment ID as defined in Section 2(1) (j) of Aadhaar (Enrolment and Update) Regulation, 2016 which means a 28 Enrolment Identification Number allocated to residents at the time of enrolment of Aadhaar.
xxiii. E-KYC authentication facility: As per in Aadhaar (Authentication) Regulations, 2016, means a type of authentication facility in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is matched against the data available in the CIDR, and the Authority returns a digitally signed response containing e-KYC data along with other technical details related to the authentication transaction;
Identity information: As per the Aadhaar Act, in respect of an individual, includes individual's Aadhaar number, biometric information and demographic information Resident: As per the Aadhaar Act, resident means an individual who has resided in India for a period or periods amounting in all to one hundred and eighty-two days or more in the twelve months immediately preceding the date of application for enrolment for Aadhaar.
Yes/No authentication facility : As defined in Aadhaar (Authentication) Regulations, 2016, means a type of authentication facility in which the identity information and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is then matched against the data available in the CIDR, and the Authority responds with a digitally signed response containing "Yes'' or "No", along with other technical details related to the authentication transaction, but no identity information.

xxiv. Definition of Money Laundering - Section 3 of the Prevention of Money Laundering (PML) Act 2002 has defined the "offence of money laundering" as "Whosoever 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."

(c) 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, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

xxv. "Group"- The term "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961 (43 of 1961). It includes a parent entity and all the entities in respect of which, for the reason of ownership or control, a consolidated financial statement for financial reporting purposes, —

(i) is required to be prepared under any law for the time being in force or the accounting standards of the country or territory of which the parent entity is resident; or (ii) would have been required to be prepared had the equity shares of any of the enterprises were listed on a stock exchange in the country or territory of which the parent entity is resident.

5.3 KYC AML CFT Policy Guidelines –

5.3.1 Customer Acceptance Policy-

(A) No account is opened in anonymous or fictitious/benami name.
(B) No account is opened where the RE is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. In case of negative CDD for existing customers, bank reserves the right to close the account based relationship with the approval of Branch Head specifying the reason thereof. (Format attached)
(C) Bank shall ensure that all the requirements are fulfilled while opening the bank accounts for disable person with autism, cerebral palsy, mental retardation and multiple disabilities (details mentioned below)
(D) In case of onboarding new customer, if any CDD relating to KYC-AML cannot be fulfilled, then such accounts should be opened as 'Small Accounts' as per prescribed guidelines (details mentioned below).
(E) The Bank may at its discretion open deposit accounts other than Current Accounts of illiterate person. The account of such person may be opened provided he/she calls on the Bank personally along with a witness who is known to both the depositor and the Bank. Normally, no cheque book facility is provided for such Savings Bank Account. At the time of withdrawal/ repayment of deposit amount and/or interest, the account holder should affix his / her thumb impression or mark in the presence of the authorized officer who should verify the identity of the person. The Bank will explain the need for proper care and safe keeping of the passbook etc. given to the account holder. In case of blind persons who are literate, ATM /Debit card, cheque book, etc. facilities will be given. The Bank official shall explain the terms and conditions governing the account.
(F) In case of customers who are blind, and wants to open an account / perform transactions, he / she is fully competent to enter into a contract like any other person. In such situations, signature or thumb impression of the blind person should be attested by an independent witness to the effect that all terms and conditions were properly explained to the blind person in his presence. Moreover, cash deposit and withdrawal by blind person should be handled by the officer of the bank. Cheque book can be issued only if the blind person can sign consistently. We should insist such customers to open an account jointly with other normal trustworthy person and mode of operation of such account should also be 'jointly' only, for operation of the account. (Format attached)

(G) No transaction or account-based relationship is undertaken without following the CDD procedure.
(H) The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation is specified below in the policy.
(I) 'Optional'/additional information is obtained with the explicit consent of the customer after the account is opened.
(J) The CDD procedure should be applied at the 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. CDD Procedure is to be followed for all the joint account holders, while opening a joint account.
(K) Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.
(L) Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.
(M) Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
(N) Where an equivalent e-document is obtained from the customer, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
(O) In the case of 'pardanashin' women, while opening a new customer, the customer should provide OVD with latest photograph and KYC documents and photograph verification should be carried out by any of female staffs of the bank.
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.
(P) The bank shall ensure that while carrying out due diligence there is no harassment to the customer. The Bank shall further ensure that the procedure adopted for due diligence shall not become too restrictive and shall not result in denial of banking services to general public, specially to those, who are financially or socially disadvantaged. Intensive due diligence shall be required for higher risk customers, especially those for whom the sources of funds are not clear.
(Q) The Bank can accept an Individual and non-individual as a customer (Resident / Non-Resident) which is in existence as per the provisions of the law.
(R) Where the bank is suspicious of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR.
(S) In case of any additional requirement from the customers, which has not been specified in the internal KYC Policy, the branches shall ensure that the same is obtained with the explicit consent of the customer.

(T) Video based Customer Identification Process (V-CIP) Certain instructions pertaining to V-CIP infrastructure and disruption in the V-CIP have been amended. Further, the requirement of 'three days' for -(i) the validity of Aadhaar XML file / Aadhaar Secure QR Code and (ii) to undertake the video process has been amended to 'three working days.

Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the RE only and all the data including video recording is transferred to the RE's exclusively owned / leased server(s) including cloud server, if any, immediately

after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the RE.

The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empaneled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.

Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the RE. However, in case of call drop / disconnection, fresh session shall be initiated.

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 three working days from the date of carrying out V-CIP.

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

(U) For particularly other type of customers or where GST number is available, the same shall be verified through the search/ verification facility provided by the issuing authority.

Guidelines for Small account

Small Account is defined in Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Sub-rule – 5) and in section 23 of KYC Master Direction, 2016.
A 'Small Account' means a savings account in which:
i. The aggregate of all credits in a financial year does not exceed rupees one lakh;
ii. The aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and
iii. The balance at any point of time does not exceed rupees fifty thousand.
iv. All such accounts should be opened for a period of 12 months only if KYC AML norms are not fulfilled.

Guideline for account of disable person with autism, cerebral palsy, mental retardation and multiple disabilities as per RBI letter 27/12.05.001/2007-08 dated 04/12/2007

The National Trust for Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 provides for a law relating to certain specified disabilities. Clause (j) of Section 2 of that Act defines a "person with disability" to mean a person suffering from any of the conditions relating to autism, cerebral palsy, mental retardation or a combination of any two or more of such conditions and includes a person suffering from

severe multiple disabilities. This Act empowers a Local Level Committee to appoint a guardian to a person with disabilities, who shall have the care of the person and property of the disabled person.

Urban Co-operative Banks (UCBs) were advised, inter alia, to rely upon the Guardianship Certificate issued either by the District Court under Mental Health Act, 1987 or by the Local Level Committees under the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999 for the purposes of opening / operating bank accounts by disabled persons with autism, cerebral palsy, mental retardation and multiple disabilities.

Local level committee has been set up in the following districts of Maharashtra -
Kolhapur, Nashik, Latur, Chandrapur, Akola, Beed, Bhandara, Nandurbar, Vardha, Gadchiroli, Thane, Amravati, Osmanabad, Satara, Buldhana, Dhule, Solapur, Ratnagiri, Gondiya, Nanded, Nagpur, Aurangabad, Yavatmal, Raigad, Mumbai Suburban, Hingoli, Pune, Sindhudurg, Ahmednagar, Sangli, Parbhani, Mumbai, Jalgaon, Jalna.

“Legal Guardianship Certificate issued under the National Trust Act, 1999 empowering the disabled persons with autism, cerebral palsy, mental retardation and multiple disabilities”

RBI have been advised by the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities (the Trust) that a question has been raised as to whether the banks and the banking sector can accept the guardianship certificates in regard to persons with disabilities issued by the Local Level Committees set up under the National Trust for the Welfare of Persons with Autism, Cerebral Palsy, Mental Retardation and Multiple Disabilities Act, 1999.

The Trust has mentioned that the above Act was specifically passed by the Parliament in order to provide for appointment of legal guardians for persons with disability that is covered under the said Act. The above Act provides for appointment of legal guardians for persons with disability by the Local Level Committees set up under the Act. The Trust has opined that a legal guardian so appointed can open and operate the bank account as long as he remains the legal guardian. It may also be noted that the provisions of Mental Health Act, 1987 also allows appointment of Guardian by District Courts.

Banks are therefore advised to rely upon the Guardianship Certificate issued either by the District Court under Mental Health Act or by the Local Level Committees under the above Act for the purposes of opening / operating bank accounts.”

As per RBI letter no. RPCD. No. RF. BC. 71/07.38.01/98-99 dated 25/02/1999 and in term of General Clauses Act, the term "sign" with its grammatical variations and cognate expressions, shall, with reference to a person who is unable to write his name, include "mark" with its grammatical variations and cognate expressions. The Supreme Court has held in AIR1950-Supreme Court, 265 that there must be physical contact between the person who signed and the signature or the mark put on the document.

An account holder, too ill to sign- cannot be physically present in the bank- can or cannot put thumb impression- due to certain physical defect or incapacity.

1. Wherever a thumb impression is obtained, it should be identified by two independent witnesses known to bank, one of whom shall be a bank official.

2. Wherever a thumb impression cannot be obtained, a mark can be obtained, (it could be toe impression as suggested), it should be identified by two independent witnesses known to the bank, one of whom shall be a bank official.

5.3.2 Customer Identification Policy (CIP) –

The Customer Identification means - identify the customer after verifying his/her identity by personal interview, independent source documents as specified by RBI guideline mentioned in Encl. Annex, data or information. Sufficient information needs to be obtained to the satisfaction, which is necessary to establish the identity of each new customer after verification in person or by supported documents' verification, whether regular or occasional, for the purpose of banking relationship. Satisfaction means to be able to satisfy the competent authorities/Bank, that due diligence was observed based on the risk profile of the customer, in compliance with the extant guidelines in place.

Customer Due Diligence (CDD) measures while commencing an account-based relationship including identifying and verifying the customer and the beneficial owner on the basis of one of the OVDs. The bank, by regulatory provisions, is required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions. During onboarding a new customer, in case of any doubts, discrepancies in the documentation / data provided by the customer, the bank will mandatorily do the customer identification process.

The bank shall undertake identification of customers in the following cases:
(i) Commencement of an account-based relationship with the customer.
(ii) Carrying out any financial transaction.
(iii) When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
(iv) 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.
(v) 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. As far as our bank is concerned, the bank will not provide any banking services / facilities to walk-in customers. Branches should urge such walk-in customers to be full-fledged customers of the bank and avail all the services offered by the bank.
(vi) When the bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
(vii) Bank shall ensure that introduction is not to be sought while opening accounts

The Customers Identity shall be verified for:

The named account holder, Beneficiary account, Signatories to an account, Intermediate parties, confirmation of business existence, For customers that are natural persons, sufficient identification data shall be obtained to verify the proof of identity of the customer, his / her address / location, his / her recent photograph.

- Documents for verifying signature- Branch Head or Branch Official shall obtain the signature of the person/customer in his / her presence for verification of signature and duly signed with code no. and bank seal.
- For customers (other than individual) that are legal persons or entities –
- Legal status of the legal person / entity shall be verified through proper and relevant documents.
- It shall be verified that any person purporting to act on behalf of the legal person / entity is so authorized to act on behalf of the legal entity. The identity of that person acting on behalf of the legal entity shall also be verified.
- Information (supportive Documents) about the ownership and control of the legal entity shall be obtained.

New customer account shall be opened with full Customer Due Diligence. If any existing customer transactions found suspicious, or when other factors shall give rise to be a belief that the customer supports to money laundering or terrorist financing, customer risk category shall be change to High risk and full scale updated Customer Due Diligence (CDD) shall be taken on record.
Customer identification data (including photograph/s) shall be periodically updated after the account is opened. The periodicity of such updation shall be once in ten years in case of low risk category customers and once in eight years in case of medium risk categories and once in two years in case of high risk categories.
Permanent correct address, means the address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other document acceptable for verification of the address of the customer.
Fresh photographs will be required to be obtained from minor customers on their becoming major.

From the date 01/04/2023 every newly opened / onboarded customer should mandatorily comply with verification of PAN card and OVD from the official website of the document issuing authorities.
KYC or other required documents which will be downloaded from government official website or official website of issuing authorities of the documents will not require the remark 'verified from original', but will require only self-attestation and remark as 'downloaded from site' which will be duly signed by authorised officer to suffice KYC compliance.

Customer Identification – Guidelines Typical cases
Walk-in Customers means- Carrying out transactions for a non-account based 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.
When a bank has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand. Identity and address of the customer shall be verified and filing a suspicious transaction report (STR) to FIU-IND may be considered.

i. Trust / Nominee or Fiduciary Accounts - There is a possibility that trust / nominee or fiduciary accounts may be used to circumvent the customer identification procedures. It shall be determined whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary. If so, receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting shall be insisted, as also shall obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, reasonable precautions shall be taken to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries shall be identified when they are defined. In the case of a 'foundation', steps shall be taken to verify the founder managers / directors and the beneficiaries, if defined.

ii. Accounts of companies and firms - Bank shall be vigilant against business entities being used by individuals as a 'front' for maintaining accounts. At the time of opening the account the bank shall verify legal status of the entity through proper and valid documents. It shall be verified that any person purporting to act on behalf of the legal entity is so authorized to act on behalf of the legal entity. The identity of the person acting on behalf of legal entity shall be verified. Information about the ownership and control of the legal entity shall also be obtained. Further, information regarding the natural person having ownership and management control over the legal entity shall be obtained. These requirements may be moderated according to the risk perception e.g. in the case of a public company, Bank may not identify all the shareholders.

iii. Client accounts opened by professional intermediaries (Pooled accounts) – If there is knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client shall be identified. 'Pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds may be maintained. 'Pooled' accounts managed by lawyers / chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients may be maintained. Where funds held by the intermediaries are not co-mingled and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners shall be identified. Where such funds are co-mingled, the beneficial owners shall be looked through. Where the 'Customer Due Diligence' (CDD) done by an intermediary is relied upon, Bank shall satisfy itself that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It may be noted that the ultimate responsibility for knowing the customer lies with the bank. Under the extant AML / CFT framework, therefore, it is not possible for professional intermediaries like Lawyers and Chartered Accountants, etc. who are bound by any client confidentiality that prohibits disclosure of the client details, to hold an account on behalf of their clients. Bank shall not allow opening and / or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc. who are unable to disclose true identity of the owner of the account / funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits Bank's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, shall not be allowed to open an account on behalf of a client.

iv. Accounts of Politically Exposed Persons (PEPs) resident outside India -

a. Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g. Heads of States or of Governments, senior politicians, senior government / judicial / military officers, senior executives of state owned corporations, important political party officials, etc. Sufficient information on any person / customer of this category intending to establish a relationship shall be gathered and all the information available of the person in the public domain shall be checked. The identity of the person shall be verified and information about the sources of funds before accepting the PEP as a customer shall be sought. The decision to open an account for a PEP shall be taken by the concerned DGM or above / concerned Regional Head. Such accounts shall be subjected to enhance monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, concerned DGM or above / concerned Regional Head shall approve to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis. These instructions are also applicable to accounts where a PEP is the ultimate beneficial owner.

b. Further, appropriate ongoing risk management procedures for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which PEP is the ultimate beneficial owner shall be applied.

c. Digital KYC Process

- The Bank will develop an application for digital KYC process which will be made available at customer touch points for undertaking KYC of their customers and the KYC process will be undertaken only through this authenticated application.
- The access of the Application will be restricted to authorized 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.
- The customer, for the purpose of KYC, shall visit the location of the authorized official or vice-versa. The original OVD shall be in possession of the customer.
- The bank will ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application will put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.
- The Application of the bank will have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.
- 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.
- The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

- 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/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.
- 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.
- 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 RE. 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.
- 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.
- The authorized officer of the bank shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.;
- 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.
- Banks may use the services of Business Correspondent (BC) for this process.

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, bank shall at their option, rely on customer due diligence done by a third party, subject to the following conditions:
(a) Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.
(b) Adequate steps are taken by REs to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence

requirements shall be made available from the third party upon request without delay.

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

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

(CIP also includes verification of certified documents from the original documents / other sources like official government websites, etc., site visits, postal confirmation, etc.)

REs may undertake V-CIP to carry out:

i) CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorised signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.

Provided that in case of CDD of a proprietorship firm, REs shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 28, apart from undertaking CDD of the proprietor.

ii) Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Section 17.

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

If opting for V-CIP, bank shall adhere to the following minimum standards:

(A) V-CIP Infrastructure

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

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

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

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

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

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

vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by suitably accredited agencies as prescribed by RBI. Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.
viii) The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, and maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

(B) V-CIP Procedure –
i) Bank will 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 RE 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 Digi Locker.

RE shall ensure to redact or blackout the Aadhaar number in terms of Section 16.

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) RE 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 RE 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 RE.
(C) V-CIP Records and Data Management
i) The entire data and recordings of V-CIP shall be stored in a system / systems located in India. REs 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.

5.3.3 KYC / CKYC / RE-KYC COMPLIANCE

i) The KYC-AML Cell will collectively work for the KYC, CKYC and RE-KYC Compliance of all the existing as well as onboarding customers. The Verification of PAN card and Aadhar card of all existing operative customers on the date 31/03/2023 will be done in a phase manner with risk wise priority as per the Quality Budget approved in the Hon. Board of Management Meeting dated _____ (Sr. No.____) Accordingly, from 01/04/2023 every newly opened/ onboarded customer should mandatorily comply with verification of PAN card and OVD from the official website of document issuing authority. KYC or other required documents which will be downloaded from government official website or official website of issuing authorities of the documents will not require the remark 'verified from original', but will require only self-attestation and remark as 'downloaded from site' which will be duly signed by authorised officer to suffice KYC compliance.

ii) Every loan proposal should comply with the KYC-AML compliance in all aspects i.e. KYC, Re-KYC, BO of LE, Risk Rating, C-KYC, of individual- other than individual (legal entity)- related persons, etc. through the condition in the loan sanction letter.

iii) As per RBI Circular dated 05/01/2023 regarding Periodic updation of KYC Details of customers, the Customer can comply with Re-KYC or KYC updation through SMS and WEBSITE for easement of KYC Updation process.
iv) Since there is backlog of huge quantum of customers pending for Re-KYC, process of CKYC for these customers is exempted for the time being during the Re-KYC process. The same is also exempted for the customers who have complied with Re-KYC through SMS or WEBSITE.

v) If the customer approaches any of the bank's branch between customer timings and complies with all KYC-AML aspects, then the Customer master in OMNI 3.0 system will be opened on the same day by CBOC department.
vi) CBOC department is responsible only for C-KYC compliance in prescribed timeframe. KYC-AML compliance will be the sole responsibility of branches, however after complying with C-KYC, if any discrepancies related to KYC-AML are detected by CBOC department, then these discrepancies will be brought to notice to branches through the 'Conditional Acceptance Portal', which will be an extra service provided by CBOC department to all branches.
vii) Customers opened/ onboarded on or after 01/04/2023 and the customers which will become due for KYC updation, will mandatorily comply with C-KYC during the process of Re-KYC and the same will be done by CBOC Department.
viii) Each customer opened/ onboarded from the date 01/04/2023 which will be due for updation should mandatorily comply with Re-KYC process with all pending KYC-AML compliance applicable to him before the customer's KYC EXPIRY DATE.
ix) The status of newly opened account under newly opened customer remains DEBIT FREEZE till its C-KYC compliance is completed and is marked as operative automatically through system post allotment of C-KYC identification unique number. The right to mark account as operative before completion of C-KYC process is given to officers ranking from AGM IT onwards.
x) In accordance with the RBI circular dated 05/01/2023, on Periodic Updation of KYC details of customers, if there is no change in KYC information and documents, a self-declaration to that effect from the individual customer is sufficient to complete the Re-KYC process. Also, Bank has provided various non face-to-face channels for that declaration i.e. registered e-mail id's, SMS, website, etc. without the need for a visit to bank branch. Further if there is change in address only, the customers can furnish revised/ updated address through any of these channels after which, bank would undertake positive verification of declared address within in two months.
xi) In accordance with the note no. 260 sanctioned by Hon. CEO dated 07/12/2022, for effective and timely compliance of Re-KYC, branches should mandatorily comply with Re-KYC process of those customers who visit branches and perform transactions or activities i.e. opening of fixed deposit, opening of another account, obtain any loan facility, SMS registration, cheque book request, net banking registration, atm card request, mobile application registration, opening of lockers, opening of d-mat accounts, performing forex transactions, etc. All the application forms required for all these activities must have the clause "no change in KYC" or "KYC compliance done" added in them.
xii) Sec. 38 sub sec. C clause Vi- "Re's should ensure that their internal KYC policy and processes on updations/periodic updations of KYC are transparent and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements." This clause is deleted from MD-KYC-2016 w.e.f 28.04.2023. In case of non-compliance of Re-KYC, the total frozen of an account, partial frozen of an account, closure of an account, customers marked as in-operative and to apply transaction restrictions to particular account or customer may be done as the case may be, for non-compliance in KYC-AML related areas. With precondition that, proper prior and detailed intimation with reasonable period should be given to customers before apply or initiates the above mentioned actions.

xiii) Aadhaar based OTP e-KYC for non-face to face mode can be used for periodic updation. Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. REs shall, however, ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

xiv) In accordance with the instructions on obligation of customers in terms of the requirements of PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account -based relationship and thereafter, as necessary, customers shall submit to the bank any updation of such documents. This shall be done within 30 days from the date of updation of the documents for the purpose of updating the records at bank's end.

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

(i) 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.

(ii) Operational Guidelines for uploading the KYC data have been released by CERSAI.

(iii) 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.

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

(v) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, bank shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above mentioned dates at the time of periodic updation as specified in Section 38 of this Master Direction, or earlier, when the updated KYC information is obtained/received from the customer.

(v) Bank shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

(vi) Where a customer, for the purposes of establishing an account based relationship, submits a KYC Identifier to our bank, with an explicit consent to download records from CKYCR, then such 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 –

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

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

(c) 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.

(d) The validity period of documents downloaded from CKYCR has lapsed.

Guidelines for Re-KYC

Re-KYC (with KYC Module Updation) for all customers –

(Updation as per Sec 38. Periodic Updation of MD KYC, 2016 updated as on 10/05/2021)
Bank should adopt a risk-based approach for periodic updation of KYC. However, periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC updation. Policy in this regard shall be documented as part of bank's internal KYC policy duly approved by our Board of Directors.

In case there is no change in the KYC document and the information contained therein obtained during customer opening or last KYC updation, then, Re-KYC declaration form available in Omni3.0 system can be used. This declaration is the sole responsibility of the customer.

With reference to the OVDs having expiry date and accepted as KYC document by the bank, then additional document field in KYC module should be updated accordingly, as the document's expiry date or KYC expiry date as per risk categorization, whichever is earlier.

As per amendment to Master Direction on KYC-2016 dated 25/02/2016 made vide RBI letter no. RBI/2021-22/35 dated 10/05/2021 the video based customer identification process (V-CIP) was introduced to simplify and rationalise the process of periodic updation.

i) **Individual Customers**:
No change in KYC information: In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the bank, customer's mobile number registered with the bank, ATMs, digital channels (such as online banking / internet banking, mobile application of bank), letter etc.
Change in address: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the bank, customer's mobile number registered with the bank, ATMs, digital channels (such as online banking / internet banking, mobile application of bank), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc. Further, the Bank, may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiii), for the purpose of proof of address, declared by the customer at the time of periodic updation.

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 us. Wherever required, we may carry out fresh KYC of such customers i.e. customers for whom account was opened when they were minor, on their becoming a major.

ii) **Customers other than individuals**:
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 us, ATMs, digital channels (such as online banking / internet

banking, mobile application of the bank), letter from an official authorized by the LE in this regard, board resolution etc. Further, we shall ensure during this process that Beneficial Ownership (BO) information available with us is accurate and shall update the same, if required, to keep it as up-to-date as possible.
Change in KYC information: In case of change in KYC information, we shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.

Additional measures: In addition to the above, the following shall be ensured
The KYC documents of the customer as per the current CDD standards are available with us. 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 us, has expired at the time of periodic updation of KYC, we shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.
Customer's PAN details, if available with us, is to be verified from the database of the issuing authority at the time of periodic updation of KYC.
Acknowledgment is to be provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out periodic updation. Further, we 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.
In order to ensure customer convenience, the facility of periodic updation of KYC is to be made available at any of our branch.
Bank should 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, and are to be adopted by our 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 RE 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 approved by the Board of Directors of our bank and decision shall be taken at the time of policy review. Bank shall ensure policy and processes on updation / periodic updation of KYC are transparent at all times and adverse actions against the customers should be avoided, unless warranted by specific regulatory requirements.

In case of existing customers, 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 bank shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer.
Provided that before temporarily ceasing operations for an account, the bank shall give the customer an accessible notice and a reasonable opportunity to be heard.
Bank may consider giving 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. Such accounts shall, however, be subject to enhanced monitoring.
Provided further that if a customer having an existing account-based relationship with the bank gives in writing to that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, then 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.
Explanation – For the purpose of this Section, "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.

KYC & Profile Updation Methods
i. Customer Contact - Under this approach, banks shall contact all customers directly through various means such as branch walk-ins, letters, emails, phone etc. asking them to furnish standard letter formats to seek customers' confirmation on the KYC records available in their database.
ii. Relationship KYC - Under this approach, any new account opened by the customer is linked to his existing relationship with the bank. E.g. a savings account customer who is more than five years old comes to open a current account. Bank identifies him as an old customer and looking at his account vintage, he is asked to furnish a fresh KYC. The KYC procedures applied at this stage may be considered as KYC updation.
iii. Surrogate Methods of KYC Updation - Some of the customer identification data available with the bank may also be verified & confirmed with independent and authentic public sources. E.g. a PAN card taken as identity proof at the time of initial KYC can be verified with the PAN number on Income Tax Website to confirm its validity and existence of the customer. Company's details can be checked from Ministry of Corporate Affairs (MCA) website. Such verification may be deemed as updation of customer identification data.
Other surrogate measures such as delivery of bank statements & deliverables to the customer's address, telephone directory search etc. may be considered as reaffirmation of his address.
Customer identification requirements in respect of a few typical cases, especially, legal persons requiring and extra element of caution are mentioned in the policy for guidance of branches.

5.3.4 LEGAL ENTITY / BENEFICIAL OWNER / LEGAL ENTITY IDENTIFIER

LEGAL ENTITY CUSTOMERS

Definition – For the purpose of beneficial ownership, legal entity customer is defined as a corporation, limited liability partnership / company, or other entity created by filing of a public document with the secretary of state or other similar office, a general partnership and any similar entity formed under law of foreign jurisdiction that opens an account.

All companies, firms, AOP, BOI, Housing societies, trusts, Ganesh Mandal, HUF etc. are included under legal entity customers i.e. in short all customers other than individual customers are treated as legal entity customers.
From 01.04.2021, for on boarding new legal entity customers, RBI has issued new templates separately for legal entity customers and related persons. Branches should mandatorily use these templates and fill every information accordingly.

Beneficial Owner (BO) – Guideline and SOP

BO declaration form -

As per RBI guidelines, declaring beneficial ownership is mandatory for legal entity customers (other than individuals). From 01/04/2021 BO declaration form is a part of customer profile form. So all branches should mandatorily comply with the same while opening of such new customers. The field is also newly introduced in customer master in OMNI3.0 and is mandatory for opening a new customer.

Policy for Beneficial ownership of legal entity customers: Identification and compliance,

Types of Beneficial Owners (BO)

i. Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.
Explanation For the purpose of this sub clause-
a. "Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.
b. "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.
ii. Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent of capital or profits of the partnership.
iii. Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.
Explanation: Term 'body of individuals' includes societies. Where no natural person identified under (i), (ii) or (iii) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.
iv. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 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.

As per Reserve Bank of India circular dated 08.09.2021 and IBA – Indian Bank Association's letter dated 16.12.2019, all customers other than individual like company account, partnership firms, trust, HUF, Body of Individuals, Association of Persons, etc. are legal entity customers and are required to declare the beneficial ownership in prescribed format. The beneficial owner is the natural person(s), who, whether acting alone or together,

or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.

In short, all customers other than individual customers are Legal entity customers and mandatory compliance regarding beneficial ownership for these customers is to get duly filled declaration form in prescribed format and fill the information in Customer master, in beneficial owners / authorised signatories field in Omni 3.0 system. For all such customers, KYC documents are mandatorily to be taken for legal entity as well as related persons and update KYC module accordingly and confirm KYC and Next KYC date as per risk categorization. Branches should verify that there is similarity in the authorised signatories (AS) and beneficial owners of legal entity customers, however there can be certain exceptions for this.

Considering the above exception, in case of difference between BO and AS, then beneficial owners should be filled first followed by authorised signatories in BO / AS field in the system. Also each name should be clearly specified as BO or AS in the system by mentioning in brackets whether the person is BO or AS. [E.g. Mr. ABC (BO), Ms CDE (BO), Mr FGH (AS), Ms IJK (AS)]

Whenever any customer submits a change in the beneficial ownership, then the entire above process needs to be mandatorily be completed right from obtaining kyc documents with customer profile form till compliance of KYC, CKYC, AML, updation in Omni 3.0.

Branches should be very careful while performing the process of Re-KYC / KYC updation that to comply with the whole beneficial ownership process as mentioned above.

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:

(a) 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.

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

LEGAL ENTITY IDENTIFIER

Introduction of Legal Entity Identifier for Large Value Transactions in Centralised Payment Systems, RBI letter no RBI/2020-21/82 DT.05/01/2021.

i. The Legal Entity Identifier (LEI) is a 20-digit number used to uniquely identify parties to financial transactions worldwide. It was conceived as a key measure to improve the quality and accuracy of financial data systems for better risk management post the Global Financial Crisis.

ii. LEI has been introduced by the Reserve Bank in a phased manner for participants in the over the counter (OTC) derivative and non-derivative markets as also for large corporate borrowers.
iii. It has now been decided to introduce the LEI system for all payment transactions of value Rs.50 crore and above undertaken by entities (non-individuals) using Reserve Bank-run Centralised Payment Systems viz. Real Time Gross Settlement (RTGS) and National Electronic Funds Transfer (NEFT).
iv. In preparation for the wider introduction of LEI across all payment transactions, member banks should:

a. advise entities who undertake large value transactions (Rs.50 crore and above) to obtain LEI in time, if they do not already have one;
b. Include remitter and beneficiary LEI information in RTGS and NEFT payment messages
c. Maintain records of all transactions of Rs.50 crore and above through RTGS and / or NEFT.

v. Entities can obtain LEI from any of the Local Operating Units (LOUs) accredited by the Global Legal Entity Identifier Foundation (GLEIF), the body tasked to support the implementation and use of LEI. In India, LEI can be obtained from Legal Entity Identifier India Ltd. (LEIL) (https://www.ccilindia-lei.co.in), which is also recognised as an issuer of LEI by the Reserve Bank under the Payment and Settlement Systems Act, 2007.
vi. These directions are issued under Section 10 (2) read with Section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007) and shall be effective from April 1, 2021.
Bank Customers who must obtain LEI are:

a. All non-individual customers initiating or receiving transactions of Rs.50 crore and above through RTGS and / or NEFT.
b. Fields in NEFT and RTGS payment messages to be used for recording Remitter and Beneficiary LEI
- For RTGS customer payment transactions, LEI information shall be provided in 'Remittance information' field.
- For NEFT outward debit messages, LEI information shall be provided in 'Sender to Receiver Information' field.

c. Technical guidelines for populating LEI in identified fields in RTGS and NEFT messages shall be communicated separately.

5.3.5 Due Diligence –

Bank shall follow 4 types of due diligence that can be used in accordance with the risk category of the customer.
A. Basic Due Diligence:
Basic Due Diligence means collection and verification of identity proof, address proof and photograph to establish the identity of the customer. This is based on documents and forms the basis of the KYC programme of the bank. A different set of documents can be listed for different type of customers as seen below in the Policy.
B. Simplified Due Diligence:

The due diligence applied to establish the identity of the customer involving measures less stringent than Basic Due Diligence, can be termed as Simplified Due Diligence. Simplified Due Diligence can be applied to Accounts of people belonging to low income group.

Simplified norms for Self Help Groups (SHGs)

(i) CDD of all the members of SHG shall not be required while opening the savings bank account of the SHG.

(ii) CDD of all the office bearers shall suffice.

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

CDD of all the members of SHG as per the CDD procedure mentioned in Section 15 of the MD shall not be required while opening the savings bank account of the SHGs.

CDD as per the CDD procedure mentioned in Section 16 of the MD of all the office bearers shall suffice. No separate CDD as per the CDD procedure mentioned in Section 15 of the MD of the members or office bearers shall be necessary at the time of credit linking of SHGs. Amendments to Master Direction – Know Your Customer (KYC) Direction -2016 – KYC norms for Self Help Groups, RBI Letter no. RBI/2021-22/10 dated 01/04/2021. As per this letter, Sec 43, clause (c) of KYC Master Direction, 2016 amended and read as "Customer Due Diligence (CDD) of all members of self-help group (SHG) may be undertaken at the time of Credit Linking of SHG's." Master direction hereby updated to reflect the changes effected by the above amendment and shall come in to force with immediate effect.

Simplified KYC norms for Foreign Portfolio Investors (FPIs)

Accounts of FPIs which are eligible/ registered as per SEBI guidelines, for the purpose of investment under Portfolio Investment Scheme (PIS), shall be opened by accepting KYC documents as detailed in Annex III, subject to Income Tax (FATCA/CRS) Rules.

Provided that banks shall obtain undertaking from FPIs or the Global Custodian acting on behalf of the FPI that as and when required, the exempted documents as detailed in Annexure.

C. Enhanced Due Diligence (EDD):

Additional diligence measures undertaken over and above the Basic Due Diligence can be termed as Enhanced Due Diligence. EDD would be required to be undertaken as per Reserve Bank of India guidelines for the medium and higher risk customers of the Bank. (For e.g. NRI, foreign Nationals, PEP, Non-face to face customer, Pooled account, Specific type of business, Customers who live in High risk countries, Trust Accounts, Correspondent Banking).

In case of situations where customers require additional due diligence in the form of EDD (Enhanced Due Diligence i.e. frequent transaction monitoring, lesser duration of KYC Updation, account to be kept under continuous observation, etc.), then the option available in KYC Updation Module in additional document field should be used to manually update next KYC date. Document field should be filled as EDD and document expiry date should be filled manually.

At branch level, while performing any transactions related to high risk customers or EDD required customers as mentioned above, there will be a pop-up displayed (alert) for both the maker and checker. "Caution – You are transacting for a High Risk / EDD required Customer". In such a situation, branch officials should carefully perform due diligence and monitor such transaction.

Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17 of KYC MD, 2016): Non-face-to-face onboarding will facilitate the bank to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section includes use of digital channels such as CKYCR, Digi Locker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. Following EDD measures shall be undertaken by the branches for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17 of KYC MD, 2016):

a) Whenever bank introduces the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP as specified in the Master Direction.

b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. Bank shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.

c) Apart from obtaining the current address proof, RE shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.

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

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

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

(The policy will be suitably amended especially for the above section i.e., on boarding of non face-to-face customers)

<u>Accounts of non-face-to-face customers (other than Aadhaar OTP based on-boarding):</u>

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

Accounts of Politically Exposed Persons (PEPs)

i. REs 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 at a senior level in accordance with the REs' Customer Acceptance Policy;

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

(e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;
(f) The CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.
ii. These instructions shall also be applicable to accounts where a PEP is the beneficial owner

Client accounts opened by professional intermediaries:
REs shall ensure while opening client accounts through professional intermediaries, that:
(a) Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.
(b) REs shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
(c) REs shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the RE.
(d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of RE, and there are 'sub-accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of RE, the RE shall look for the beneficial owners.
(e) REs shall, at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.
(f) The ultimate responsibility for knowing the customer lies with the RE.

EDD for customers' transactions in Virtual Currencies –

As per RBI circular dated 18.04.2018, RBI had prohibited entities regulated by it to not deal in VCs or provide services for facilitating any person or entity in dealing with or settling VCs. Such services include maintaining accounts, registering, trading, settling, clearing, giving loans against virtual tokens, accepting them as collateral, opening accounts of exchanges dealing with them and transfer / receipt of money in accounts relating to purchase/ sale of VCs. The above circular was set aside by the Hon'ble Supreme Court on March 04, 2020 and as such the above RBI circular was stated invalid from the date of Hon. Supreme Court order. This was specifically mentioned by RBI in its circular dated 31.05.2021.

In view of the said above circular, bank shall continue to provide banking services to such customers subject to positive enhanced due diligence and classifying the same into high risk category.

D. **On-going Due Diligence (ODD):**

Ongoing due diligence with respect to the business relationship with every client shall be exercised and the transactions shall be examined closely in order to ensure that they are consistent with the banks knowledge of the client, his business and risk profile and where necessary, the source of funds. REs 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.

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

- Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
- Transactions which exceed the thresholds prescribed for specific categories of accounts.
- High account turnover inconsistent with the size of the balance maintained.
- Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

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

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

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.

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.

Branches should carry out on-going due diligence of existing customers which is regular monitoring of transactions in accounts in order to ensure that their transactions are consistent with the branch's knowledge of the customer, his business and risk profile and wherever necessary, the source of funds.

Bank should consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML), wherever possible, to support effective monitoring for ongoing due diligence. Bank should try to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements (sec 54A).

Customer Due Diligence (CDD) Procedure –

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

(i) the Aadhaar number where,

(a) 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

(b) he decides to submit his Aadhaar number voluntarily to a bank or any RE notified under first proviso to sub-section (1) of section 11A of the PML Act; or

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

(b) 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; or

(c) The Bank can obtain KYC Identifier with explicit customer consent to download KYC records from CKYCR, for the purpose of CDD (as per amended Section 16): and

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

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

Provided that where the customer has submitted,

a) Aadhaar number under clause (a) above to a bank or to a RE notified under first proviso to sub-section (1) of section 11A of the PML Act, such bank or RE shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the RE.

b) proof of possession of Aadhaar under clause (aa) above where offline verification can be carried out, the RE shall carry out offline verification.

c) an equivalent e-document of any OVD, the RE 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 in digital KYC annexure.

d) any OVD or proof of possession of Aadhaar number under clause (ab) above where offline verification cannot be carried out, the RE shall carry out verification through digital KYC.

e) KYC Identifier under clause (i-c) above, the RE shall retrieve the KYC records online from the CKYCR in accordance with Section 56.

Provided that for a period not beyond such date as may be notified by the Government for a class of REs, instead of carrying out digital KYC, the RE 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, REs 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 RE and such exception handling shall also be a part of the concurrent audit as mandated in Section 8. REs 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 RE and shall be available for supervisory review.

Explanation 1: RE 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 as per proviso (i) above.

Explanation 2: Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators.

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.
Accounts opened using OTP based e-KYC, in non-face-to-face mode, are subject to the following conditions:

- There must be a specific consent from the customer for authentication through OTP.
- 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.
- the aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.
- 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.
- Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 16 or as per Section 18 (V-CIP) is carried out. If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication.
- 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.
- 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 RE. Further, while uploading KYC information to CKYCR, REs 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. REs 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.

Accounts of non-face-to-face customers – Accounts of non-face-to-face customers with the introduction of telephone and electronic banking, increasingly accounts are being opened for customers without the need for the customer to visit the Bank Branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, adequate procedures to mitigate the higher risk involved shall be applied. The bank shall insist upon Certification of all the documents presented and, if necessary, additional documents shall be called for. In such cases, first payment shall be effected through the customer's account with another Bank which in turn, adheres to similar KYC standards.

CDD Measures for Opening of bank accounts (Individuals)– The Bank shall apply following procedure while establishing an account based relationship with an individual A) Obtain information as mentioned under sec 15 and b) such other documents pertaining to the nature of business or financial status specified by the bank, provided that information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged (disclosed) for the purpose of cross selling, or for any other purpose without the express permission of the customer.

CDD Measures for Opening of bank accounts (Non- Individuals)– CDD measures in case of certain categories of non- individual customers, the CDD measures pertaining to the following categories of non-individual customers have been amended to include certain additional information/document requirements,

CDD procedure, including Aadhaar authentication and obtaining PAN/form 60as applicable, shall be carried out for all the joint account holders.

Salaried Employees It has been brought to our notice that for opening bank accounts of salaried employees some banks rely on a certificate / letter issued by the employer as the only KYC document for the purposes of certification of identity as well as address proof.

Such a practice is open to misuse and fraught with risk. It is, therefore, clarified that with a view to containing the risk of fraud, banks need to rely on such certification only from corporates and other entities of repute and should be aware of the competent authority designated by the concerned employer to issue such certificate/letter.

Further, in addition to the certificate from employer, banks should insist on at least one of the officially valid documents as provided in the Prevention of Money Laundering Rules (viz. passport, driving license, PAN Card, Voter's Identity card etc.) or utility bills for KYC purposes for opening bank account of salaried employees of corporates and other entities.

In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and third party certification / introduction may have to be relied on. In such cases, it shall be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

CDD Measures for Sole Proprietary firms

For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out. Apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, the following documents shall be called for and verified before opening of accounts in the name of proprietary concern:

In addition to the above, any two of the following documents or the equivalent e-documents there of as a proof of business/ activity in the name of the proprietary firm 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 REs are satisfied that it is not possible to furnish two such documents, REs may, at their discretion, accept only one of those documents as proof of business/activity.

Provided REs undertake contact point verification and collect 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.

Section 28 has been amended to clarify that "Registration certificate" as a proof of business/ activity in the name of the proprietary firm includes "Udyam Registration Certificate (URC) issued by the Government".

CDD Measures for Legal Entities

A. **For opening an account of a company**, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
(i) Certificate of incorporation
(ii) Memorandum and Articles of Association
(iii) Permanent Account Number of the company
(iv) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
(v) Documents, as specified in Section 16, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf
(vi) the names of the relevant persons holding senior management position; and
(vii) the registered office and the principal place of its business if it is different.

B. **For opening an account of a partnership firm**, the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
(i) Registration certificate
(ii) Partnership deed
(iii) Permanent Account Number of the partnership firm and
(iv) Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
(v) the names of all the partners and
(vi) address of the registered office, and the principal place of its business, if it is different.

C. **For opening an account of a trust**, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
(i) Registration certificate
(ii) Trust deed
(iii) Permanent Account Number or Form No.60 of the trust (As per IBA letter 02 June 2021 – In terms of sec 9 (8) (iii) of PML Rules, 2005 PAN or Form 60 must be collected from the trust at the time of establishing an account based relationship.)
(iv) Documents, as specified in Section 16, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.
(v) the names of the beneficiaries, trustees, settlor and authors of the trust
(vi) the address of the registered office of the trust; and

(vii) list of trustees and documents, as specified in Section 16, for those discharging the role as trustee and authorised to transact on behalf of the trust.

D. **For opening an account of an unincorporated association or a body of individuals**, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
(i) Resolution of the managing body of such association or body of individuals
(ii) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals
(iii) Power of attorney granted to transact on its behalf
(iv)Relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and Documents, as specified in Section 16,
(v) Such information as may be required by the RE to collectively establish the legal existence of such an 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.

E. **For opening accounts of judicial persons** not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents or the equivalent e-documents thereof shall be obtained:
(i) Document showing name of the person authorised to act on behalf of the entity;
(ii) Documents, as specified in Section 16, of the person holding an attorney to transact on its behalf and
(iii) Such documents as may be required by the RE to establish the legal existence of such an entity/juridical person.

F. **Procedure to be followed by banks while opening accounts of foreign students**
(i) Banks shall, at their option, open a Non-Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.
a. Provided that a declaration about the local address shall be obtained within a period of 30 days of opening the account and the said local address is verified.
b. Provided further that pending the verification of address, the account shall be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of rupees fifty thousand on aggregate in the same, during the 30-day period.
(ii) The account shall be treated as a normal NRO account and shall be operated in terms of Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of FEMA 1999.
(iii) Students with Pakistani nationality shall require prior approval of the Reserve Bank for opening the account.

5.3.6 Risk Management –
5.3.6.1 - Risk Identification, Measurement, Mitigation and Review Mechanism –
5.3.6.2 - Risk Categorization of the Customers
5.3.6.3 - Risk Assessment of the Bank

5.3.6.1 Risk Identification, Measurement, Mitigation and Review Mechanism (As per Risk management Committee requirement for AML Cell) –

AML Cell hereby tries to identify and mitigate the risks in the working of the department at HO level and also at branch level. Accordingly following are the major risks identified.

Bank is exposed to the following risks which arise out of Money Laundering activities and non-adherence of KYC standards.
i. **Reputation Risk** - Risk of loss due to severe impact on Bank's reputation. This may be of particular concern given the nature of the Bank's business, which requires the confidence of depositors, creditors and the general market place. This might happen because of –
'Wrong reporting of genuine customer transactions as suspicious',
'Customers are harassed in complying process of KYC AML guidelines', etc.
ii. **Compliance Risk** - Risk of loss due to failure of compliance with key regulators governing the Bank's operations. The risk may arise because of –
'Supervisory action imposed by RBI followed by imposition of monetary penalty due to non-compliance of regulatory obligations',
'Lacunae in systems and procedures', etc.
iii. **Operational Risk** - Risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. The risk may arise due to situations like –
'Lack of proper training to departmental and branch staff',
'No proper operating procedures as per regulatory guidance'
iv. **Legal Risk** - Risk of loss due to any legal action the Bank or its staff may face due to failure to comply with the law. Bank may face such risk because of -
'Non adherence of mandatory laws',
'Complaint registered by customers related to KYC AML issues', etc.

Mitigation of risks –
Thorough scrutiny of suspicious transactions should be done with application of mind and should be reported only after taking due care that genuine customers are not reported. No customer should be harassed for complying with KYC AML guidelines. (This is also mentioned separately in the policy), moreover various technological means should be provided to the customers for timely compliance. Bank is also trying to create awareness among customers related to KYC AML norms.
Bank has developed strong SOPs and policy documents in adherence with regulatory guidelines and related laws supported with effective and repeated training programs to all concerned staff working in department and branch to mitigate all the above risks.

For the purpose of effective implementation of KYC policy and AML standards, Anti Money Laundering Cell headed by the Principal Officer with the need based help of branches shall monitor transactions in all customer accounts on concurrent basis with the help of AML software and IT support to meet the requirements of KYC / AML policy and standards.

For instance, checking of negative list at the time of account opening, monitoring of transactions in customer accounts based on customer profile, customer type, nature of business / profession, number and value of transactions, different types of transactions, monthly turnover in the account, very large / suspicious transactions, transactions in new / dormant accounts etc. and draw various reports from historic data based on parameters defined etc.
All transactions of suspicious nature shall be reported to Principal Officer as and when the transactions are found to be suspicious by the branches. The Principal Officer of the Bank shall ensure that such reporting system is in place and shall monitor receipt of the reports and onward submission to FIU-IND as per legal requirement.

Introduction of new technologies – All the departments should ensure that they should identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products and shall undertake the risk assessments prior to the launch or use of such products, practices, services and technologies; and adopt risk-based approach and adhere with KYC-AML norms to manage and mitigate the risks through appropriate EDD measures (wherever applicable) and transaction monitoring, etc.

The Executive Committee on KYC and AML shall review and set up various limits relevant for KYC and AML standards.

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

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

Provided that various other information collected from different categories of customers relating to the perceived risk, is non-intrusive and the same is specified in the KYC policy.
Explanation: FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), guidance note circulated to all cooperative banks by the RBI etc., may also be used in risk assessment.

(i) Before opening a new account, necessary checks shall be conducted so as to ensure that the identity of the customer does not match with any person with known criminal

background or with banned entities such as individual terrorists or terrorist organizations etc.

(ii) A list circulated by RBI of persons with known criminal background or banned entities as well as a list of persons involved in frauds and deliberate default as per information available with the Bank shall be used for this purpose.

(iii) For the purpose of risk categorization of customer, the relevant information shall be obtained from the customer at the time of account opening. The bank shall ensure that information sought from the customer is relevant to perceived risk and is not intrusive. Any other information from the customer shall be sought separately with his / her consent and after opening the account.

(iv) Initial Risk perception of different types of customers shall be decided based on the relevant information provided by the customer at the time of account opening. The account shall be classified under proper risk category accordingly. (Indicative list of Customer account type & required risk category is enclosed for ready reference (Annex II)

(v) The information based on the following aspects shall be obtained for preparing the customer profile and deciding the risk categorization of the account

- Background to the customer, Customer's identity,
- Social/financial status.
- nature of business activity,
- location of customer
- activity and profile of his / her clients,
- country of origin,
- sources of funds,
- mode of payments,
- Volume of turnover, etc.

(vi) The formats for obtaining information as per initial risk categorization shall be devised by the bank.

(vii) The Executive Committee shall be the competent authority to approve the aspects to be considered required for preparing the Customer Risk Profile. An indicative risk categorization of customers based on customer types is provided in KYC AML Procedures which shall be reviewed periodically by the Executive Committee for KYC AML in the light of Government / Regulators Guidelines.

(viii) Customer Risk Profiling - A profile for each new customer shall be prepared based on initial risk categorization. The customer risk categorization shall be carried out as per procedure mentioned in KYC AML procedures. The customer profile shall generally contain information which shall be helpful to the bank during the transaction monitoring for the purpose of reporting of STR as per Obligations of the bank under PMLA. The nature and extent of due diligence shall depend on the risk categorization of the customer.

(ix) The bank while preparing Customer risk profile shall seek only such information which is relevant to the risk category and is not intrusive. The customer profile shall be a confidential document. The information contained in the document shall only be shared within the bank on need to know need to do basis. The Customer Risk Profile information and details contained therein shall not be shared to any outside party unless mandated under any statutory or legal obligation.

(x) The customer risk profile shall not be divulged for cross selling or any other purposes.

(xi) Indicative information to be obtained from the customer at the time of opening of account for the purpose of creating customer profile is given in KYC AML Procedures. The

information to be sought from the customer shall be as per the customer risk categorization reviewed by Executive Committee on KYC and AML from time to time based on the guidelines issued by RBI / Bank and also depending upon business requirement and composition of the customers.

(xii) Customers shall be accepted after completion of all the steps as required by the Customer Identification Procedures of the bank.

(xiii) The required documents and other information shall be collected in respect of different categories of customers depending on the risk perception.

(xiv) Indicative list of documents required to be submitted by the customer at the time of opening of account is given in KYC AML Procedures. This list of documents to be obtained from the customers shall be reviewed from time to time by the Executive Committee for KYC and AML based on emerging business needs and guidelines issued by RBI / Bank.

(xv) Circumstances, in which a customer shall be permitted to act on behalf of another person / entity, as there shall be occasions when an account is to be operated by an intermediary in fiduciary capacity, shall also be spelt out in KYC AML Procedures. Customer Due Diligence (CDD) Procedure is followed for all the joint account holders, while opening a joint account.

(xvi) The bank shall ensure that parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorization of customers into low, medium and high risk (banks may choose any suitable nomenclature viz. level I, level II and level III). Customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs) may, if considered necessary, be categorized even higher;

(xvii) The bank shall ensure documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and instructions/guidelines issued by Reserve Bank from time to time;

(xviii) For the purpose of risk categorisation, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorised as low risk. Illustrative examples of low risk customers could be 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 and Government owned companies, regulators and statutory bodies etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met.

Customers that are likely to pose a higher than average risk to the bank should be categorised as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc.

Banks should apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive ‘due diligence’ for higher risk customers, especially those for whom the sources of funds are not clear.

Examples of customers requiring higher due diligence include (a) non-resident customers; (b) high net worth individuals; (c) trusts, charities, NGOs and organizations receiving donations; (d) companies having close family shareholding or beneficial ownership; (e) firms with ‘sleeping partners’; (f) politically exposed persons (PEPs) of foreign origin; (g) non-face to face customers and (h) those with dubious reputation as per public information available

etc. However only NPOs/NGOs promoted by United Nations or its agencies may be classified as low risk customer. It is important to bear in mind that the 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.

We can take a review of the risk parameter of these customers at the time of risk assessment of the bank, as per sec. 5A of MD on KYC-2016 dated 25/02/2016 amended time to time, latest on 04/05/2023.

5.3.6.3 Risk Assessment of the Bank –

Internal ML/TF risk assessment by REs - Amendment to Master Direction (MD) on KYC
The Master Direction on KYC dated February 25, 2016, is hereby updated to reflect the following changes in line with Rule 9(13) of the PML Rules 2005:
a) A new section (5A) has been added to chapter II of the MD on KYC requiring REs 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, REs 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 RE shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the RE. Further, the periodicity of risk assessment exercise shall be determined by the Board of the RE, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least twice in a year.
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) REs 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, REs shall monitor the implementation of the controls and enhance them if necessary.
KYC verification once done by one branch/office of the RE shall be valid for transfer of the account to any other branch/office of the same RE, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.
e) In accordance with the confidential letter issued by RBI dated 25/05/2021, 20/03/2023 and 03/04/2023, the Risk Assessment of the Bank should include-
1] Risk based approach
2] Outcomes of abridged version of National Risk Assessment-2022 (NRA)
3] KYC-AML-CFT compliance according to FATF mutual evaluation

Risk assessment of the bank along with its review will be taken on yearly basis, immediately after completion of every financial year. The detail report with assessment of each year should be kept by the end of June of the following year.

Guideline for Bank's risk assessment and risk management & its review: (as per KYC MD 2016 dt. 25/02/2016 para no. 5A added in line with rule 9(13) of the PML Rule 2005.)

Main objective is to identify, assess risk and to take effective measures to mitigate the ML/TF risk for clients, geographical areas, products, services, transactions or delivery channels.

To identify and assess banks ML/TF risk following factors to be considered,

Geographical Presence: Identify total districts where branches are located. District wise points should be given out of 10 as per risk (1-4 low risk, 5-7 medium risk and 8-10 high risk). Average to be calculated for all the districts together and then final risk rating to be given as Bank's Geographical Presence Risk Rating as per above matrix.

Customer Base: (i) Total customers to be bifurcated in 'Individual' and 'Other' categories. Percentage of Individual customers to total customers will decide the points. If percentage is between 1-100%, then points should be given from 1 to 10 (i.e. higher the percentage, lower the points) and percentage of other customers to total customers will decide the points. If percentage is between 1-20% then points to be given from 1 to 10 (i.e. higher the percentage, higher the points)

Average of '(i)' will be as - below 40 % low risk, between 41 to 70 % medium, between 71 to 100 % high risk

(ii)Total customers also bifurcated as per risk categorization as low, medium, high in Omni 3.0 system. Percentage of every risk customers (i.e. low risk, medium risk and high risk) to total customers and points should be given from as per risk wise percentage. Process to be followed as below –

For Low Risk Customers – If percentage of low risk customers is between 20-100% then points to be given from 1 to 10 (i.e. higher the percentage, lower the points)

For Medium Risk Customers - If percentage of medium risk customers is between 1-20% then points to be given from 1 to 10 (i.e. higher the percentage, higher the points)

For High Risk Customers - If percentage of high risk customers is between 1-10% then points to be given from 1 to 10 (i.e. higher the percentage, lower the points)

Average of '(ii)' will be as - below 40 % low risk, between 41 to 70 % medium, between 71 to 100 % high risk

Average of (i) and (ii) above will decide Bank's Customer Base Risk Rating as per above matrix. (Below 4 low risk, 5-7 medium risk and above 8 high risk)

KYC Compliance: For Risk rating for this factor, all factors such as KYC, RE-KYC, C-KYC, and compliance of BO of LE customers are to be considered. Risk wise pendency percentage decides the risk categorization and points accordingly. Up to 40% pendency will be low risk with 1 to 4 marks, 41 to 70% pendency will be medium risk with 5 to 7 marks and 81 to 100% pendency will be high risk with 8 to 10 marks. Average of all above will decide Bank's KYC Compliance risk rating as per above matrix.

Transaction Base: (i) Total transactions to be bifurcated as system transactions (cash, transfers, RTGS, NEFT made at branch level) and digital transactions (RTGS NEFT, netbanking, UPI, IMPS, mobile apps, QR code etc. made using digital platform) percentage of digital transactions decides the risk categorization and points accordingly. Up to 40% digital transactions will low risk and 1 to 4 marks, 41 to 70% digital transactions will medium risk and

5 to 7 marks, 81 to 100% digital transactions will high risk and 8 to 10 marks. Average of all above earn out of 10 marks.

(ii) Total transactions also to be bifurcated amount wise. Up to 10 lac low, up to 50 lac medium, above 50 lac high. Risk category having amount more than 50% will decide the risk category and earn points accordingly, i.e. higher the percentage lower the points for low risk, higher the percentage higher the points for medium and high risk.

Average of (i) and (ii) will decide Bank's Transaction base risk rating as per above matrix.

Amount Base: (i) All advances to be bifurcated amount wise, up to 50 lac low risk, up to 500 lac medium risk, above 5 cr high risk. Risk category having amount more than 50% will decide the risk category and earn points accordingly, i.e. higher the percentage lower the points for low risk, higher the percentage higher the points for medium and high risk.

(ii.a) All deposits to be bifurcated amount wise, up to 50 lac low risk, from 5000001 up to 500 lac medium risk, above 5 cr high risk. Risk category having amount more than 50% will decide the risk category and earn points accordingly, i.e. higher the percentage lower the points for low risk, higher the percentage higher the points for medium and high risk.

(ii.b) All term deposits to be bifurcated maturity / age wise, within 1 year high risk, from 1 year to 3 years medium risk, above 3 years low risk. Risk category having maturity more than 50% will decide the risk category and earn points accordingly, i.e. higher the percentage lower the points for low risk, higher the percentage higher the points for medium and high risk.

Average of (i) and (ii) will decide Bank's Amount base risk rating as per above matrix.

Product Base: (i) For advances, required product wise bifurcation and its overdue amounts for consideration. Every product gets risk rating according to its overdue percentage, and points given accordingly. (i.e. overdue below 5% low risk and points 1 to 4, overdue 6 to 10% medium risk and points 5 to 7, overdue over 10% high risk and points 8 to 10) Average for the above is risk category for advances and points given accordingly.

(ii) For deposits, as per nature and possibility of transaction complexity, all current accounts are high risk, all saving product accounts are medium risk, all term deposits are low risk, and bifurcation should be made accordingly. Amount wise majority percentage is risk category for deposits and points to be given accordingly.

Average of (i) and (ii) will decide Bank's product base risk rating as per above matrix.

Above mentioned process of Risk assessment especially regarding ML/TF concerns deal with major Risks namely operational risk, Business risk, Compliance risk, Reputation risk, liquidity risk, and we can easily identify the highlighted areas with quantum and intensity.

We should adopt following measures to mitigate those Risks -

1. Apply Enhance due diligence process where required,
2. Effective risk categorization and risk migration,
3. Prioritization for pendency work compliance,
4. Curtailment of intervals for required Audits, where ever necessary,

Bank's risk assessment and risk management process, should be done at least once in six calendar months. Detailed report for the same with highlighted effective measures taken to mitigate the ML/TF risk, to be kept in the next month's Hon. ACB meeting.

The whole process should be reviewed annually and recommendations to be made by the office to take necessary steps or changes in process. All recommended and sanctioned changes in process should come into existence with immediate effect from sanction date of

the note. All the required data and reports for the above assessment process is to be taken from MIS Dept. and Data Center.

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

Under FATCA and CRS, REs 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 and if so, shall take following steps for complying with the reporting requirements:

(i) Register on the related e-filling portal of Income Tax Department as Reporting Financial Institutions at the link https://incometaxindiaefiling.gov.in/ post login --> My Account --> Register as Reporting Financial Institution,

(ii) 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: REs 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.

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

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

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

(v) 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. REs may take note of the following:

a. updated Guidance Note on FATCA and CRS

b. a press release on 'Closure of Financial Accounts' under Rule 114H (8).

5.3.8 - OBLIGATIONS UNDER PMLA 2002

In accordance with the RBI Circular No. RBI/2023-24/24 dated 28/04/2023 regarding amendment to the Maste Directions on KYC 2016, the proposed changes and amendments in the Prevention of Money Laundering Act, 2002 are as follows:-

- Introduction:

In order to prevent banks and other financial institutions from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of

the financial system, efforts are continuously being made both internationally and nationally, by way of prescribing various rules and regulations.

Internationally, the Financial Action Task Force (FATF) which is an inter-governmental body established in 1989 by the Ministers of its member jurisdictions, sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. India, being a member of FATF, is committed to upholding measures to protect the integrity of international financial system.

In India, the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, form the legal framework on Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT).

- Scope:

REs' policy framework should seek to ensure compliance with PML Act/Rules, including regulatory instructions in this regard and should provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, REs may also consider adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

- Access to information (as per Section 12A of PMLA):

(1) The Director may call for from any reporting entity any of the records referred to in [section 11A, sub-section (1) of section 12, sub-section (1) of section 12AA

and any additional information as he considers necessary for the purposes of this Act.

(2) Every reporting entity shall furnish to the Director such information as may be required by him under sub-section (1) within such time and in such manner as he may specify.

(3) Save as otherwise provided under any law for the time being in force, every information sought by the Director under sub-section (1), shall be kept confidential.

- Enhanced due diligence (as per section 12AA of PMLA – Specified Transactions):

(1) Every reporting entity shall, prior to the commencement of each specified transaction,

(a) verify the identity of the clients undertaking such specified transaction by authentication under the Aadhaar in such manner and subject to such conditions, as may be prescribed: Provided that where verification requires authentication of a person who is not entitled to obtain an Aadhaar number under the provisions of the said Act, verification to authenticate the identity of the client undertaking such specified transaction shall be carried out by such other process or mode, as may be prescribed;

(b) take additional steps to examine the ownership and financial position, including sources of funds of the client, in such manner as may be prescribed: -

(c) take additional steps as may be prescribed to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties.

(2) Where the client fails to fulfill the conditions laid down under sub-section (1), the reporting entity shall not allow the specified transaction to be carried out.

(3) Where any specified transaction or series of specified transactions undertaken by a client is considered suspicious or likely to involve proceeds of crime, the reporting entity shall increase the future monitoring of the business relationship with the client, including greater scrutiny or transactions in such manner as may be prescribed.

(4) The information obtained while applying the enhanced due diligence measures under sub-section (1) shall be maintained for a period of five years from the date of transaction between a client and the reporting entity,

Explanation. — Specified transaction value is to be considered as Rs. 10 Crores which constitutes-

(a) any withdrawal or deposit in cash, exceeding such amount.

(b) any transaction in foreign exchange, exceeding such amount.

(c) any transaction in any high value imports or remittances.

(d) such other transaction or class of transactions, in the interest of revenue or where there is a high risk or money-laundering or terrorist financing, as may be prescribed.

- Civil Criminal Proceeding against Bank, its directors, its employees in certain cases – (Section 14 of PMLA):

No civil or criminal proceedings against reporting entity, its directors and employees in certain cases. —Save as otherwise provided in section 13, the reporting entity, its directors and employees shall not be liable to any civil or criminal proceedings against them for furnishing information under clause (b) of sub-section (1) of section 12.

Section 12 of PML Act 2002 issued by the Central Government, Ministry of Finance, Department of Revenue vide their notifications dated July 1, 2005 and subsequent notification, places certain obligations on every banking company, financial institution and intermediary, which include;

5.3.8.1 Maintenance of records of transactions
5.3.8.2 Information to be preserved
5.3.8.3 Maintenance and preservation of record
5.3.8.4 Reporting to Financial Intelligence Unit – India
5.3.8.5 Monitoring of Transactions

5.3.8.1 - Maintenance of records of transactions:

As per the PML Act, proper record of transactions prescribed under Rule 3 of PML Act shall be maintained properly by the bank.

Details of transactions required to be kept as under PML Act are as under:
i) All cash transactions of the value of more than Rs.10.00 lakhs or its equivalent in foreign currency.
ii) All series of cash transactions integrally connected to each other, which have been valued below Rs.10.00 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rs.10.00 lakhs.
iii) All transactions involving receipts by non-profit organisations of value more than Rs.10.00 lakhs or its equivalent in foreign currency.
iv) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or documents has taken place facilitating the transactions.
v) All suspicious transactions whether or not made in cash and by way of cheques including third party cheques, pay orders, demand drafts, cashier cheques, travelers cheques, account transfers, credits or debits into or from any non-monetary accounts (shares, demat accounts), money transfer or remittance, loans and advances, collection services etc.

5.3.8.2 - Information to be preserved

(a) As per the PML Act, all necessary information in respect of transactions referred to in Rule 3 of PML Act has to be maintained properly, to permit reconstruction of individual transaction, including the following information:
i) The nature of the transaction
ii) The amount of transaction and the currency in which it was denominated
iii) The date on which the transaction was conducted
iv) The parties to the transaction
(b) Evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;
(c) Maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

5.3.8.3 - Maintenance and Preservation of Record –

i. Records containing information of all transactions including the records of transaction detailed in Rule 3 has to be maintained.
ii. Data to be preserved in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. Records to be maintained for 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 shall permit reconstruction of individual transactions (including the amount and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.
iii. Records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended. The identification records and transaction data shall be made available to the competent authorities upon request.

iv. Background including all documents / office records/ memorandums pertaining to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose and purpose thereof shall, as far as possible, be examined and the findings at branch as well as Principal Officer level to be properly recorded. Such records and related documents to be made available to help auditors in their day-to-day work relating to scrutiny of transactions and also to Reserve Bank / other relevant authorities. These records are required to be preserved for five years as is required under PMLA, 2002.

Record Management -
As per section 12 of PMLA - Reporting entity to maintain records: —

(1) Every reporting entity shall—(a) maintain a record of all transactions, including information relating to transactions covered under clause (b) in such manner as to enable it to reconstruct individual transactions; (b) furnish to the Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed; (c) maintain record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.

(2) Every information maintained, furnished or verified, save as otherwise provided under any law for the time being in force, shall be kept confidential.

(3) The records referred to in clause (a) of sub-section (1) shall be maintained for a period of five years from the date of transaction between a client and the reporting entity.

(4) The records referred to in clause (e) of sub-section (1) shall be maintained for a period of five years after the business relationship between a client and the reporting entity has ended or the account has been closed, whichever is later.

(5) The Central Government may, by notification, exempt any reporting entity or class of reporting entities from any obligation under this Chapter.

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

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

5.3.8.4 - Reporting to FIU-INDIA –

The bank shall strictly follow the time schedule given by the regulators (FIU-IND/ RBI/Government of India etc.) for submission of mandatory reports, so as to avoid any unpleasant instances of penal actions. The Principal Officer shall ensure /supervise/monitor the report submission. The Principal Officer shall be the authorised signatory for giving authentication on behalf of the bank for submission of reports.

i. **Cash Transaction Report (CTR)** - The Cash Transaction Report (CTR) for each month shall be submitted to FIU-IND within the time schedule prescribed by the regulators (FIU-IND).

For submission of CTR, details of individual transactions below rupees Fifty Thousand need not be furnished.

CTR shall contain only the transactions carried out on behalf of clients / customers excluding transactions between the internal accounts of the bank.

The bank shall use the AML application OMNI Enterprise procured by the bank (developed by M/S Infrasoft) for generation of Cash Transaction Reports.

The AML cell shall generate the mandatory reports as per the prescribed periodicity.

Any changes in AML Application required due to the change in the regulators requirements / guidelines, shall be immediately informed by the AML cell to the I T Department.

The IT Department shall be responsible to get the necessary changes / modifications done from the vendor on receipt of requirements from the AML Cell.

The cash transaction report for the Bank as a whole shall be submitted by the Principal Officer.

The guidelines / instructions on 'Maintenance of records of transactions', 'Information to be preserved' and 'Maintenance and Preservation of records' shall be issued by the AML Cell. The branches shall scrupulously / strictly follow the guidelines regarding the maintenance of records.

ii. **The Counterfeit Currency Report CCR** - All cash transactions where forged or counterfeit Indian currency notes have been used as genuine shall be reported by the Principal Officer to FIU-IND in the specified format as per the time schedule specified by the regulators.15th of next succeeding month.

These cash transactions shall also include the transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text format.

iii. **Suspicious Transaction Report (STR)**

a) The decision to report any transaction as a Suspicious Transaction shall be taken by the STR Committee constituted for AML headed by Principal Officer.

b) The Suspicious Transaction Report on behalf of the Bank shall be submitted by the Principal Officer.

c) While deciding transactions as suspicious, banks shall be guided by definition of suspicious transaction contained in Prevention of Money Laundering Act & Rules as amended from time to time. Final authority to report transactions as suspicious lies with the Principal Officer.

d) In some cases, transactions may be abandoned / aborted by customers on being asked to give details or to provide documents. All such attempted transactions shall be reported in STRs, even if not completed by the customers, irrespective of the amount of the transaction.

e) STRs shall be made if there are reasonable grounds to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction.

f) The Suspicious Transaction Report (STR) shall be furnished as per the time schedule prescribed by the regulators. (Presently within 7 days of arriving at a conclusion that the transaction is suspicious). The Principal Officer shall record reasons for treating any transaction or a series of transactions as suspicious.
g) It shall be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report shall be made available to the competent authorities on request.
h) All cash or non-cash transactions or a series of transactions integrally connected shall be reported if found to be of suspicious nature.
i) In the context of creating KYC / AML awareness among the staff and for generating alerts for suspicious transactions, Bank shall consider the indicative list of suspicious activities contained in Annex –D to the IBA's Guidance Note for Banks, 2009.
j) No restrictions shall be put on operations in the accounts where an STR has been submitted. The fact of furnishing of STR shall be kept strictly confidential, as required under PML Rules. Customer shall not be tipped off at any level.
k) FIU-INDIA Have given guidelines on dt. 28/09/2020 for effective detection and reporting of suspicious transactions with a) Monitoring scenario thresholds setting & tuning b)Model templates for STR's (GOS part) and filing STRs. c) Model templates for STR's (GOS part) and filing STRs.- clarification.
l) In view of FIU-IND circular dated 11.05.2021, bank should refrain from only reporting STR only based on number of transactions made through UPI. (e.g. 18 debit transactions and 6 credit transactions, so found suspicious). Along with the number of transactions, ground of suspicion (GoS) must also include details of underlying bank accounts from where credit through UPI is received in the reported account or debit through UPI is made from the reported account while reporting STRs. Value of such transactions, volume of transactions and frequency should also be mentioned in GoS. Deviance from this circular may attract monetary penalty u/s 13 of PMLA, 2002.
m) Generation, scrutiny and reporting / clearance of all online VRV alerts will be mandatorily done at Branch level. Alerts amounting to Rs. 25 lac and above should be secondarily scrutinised and further reporting / clearance to be done at head office level. Generation, scrutiny and clearance of offline VRV and SDN alerts will be done at branch level and reporting of suspicious customers will be done at HO Level. Record keeping will be done at HO level and branch level for respective alerts.

Before opening any new account, the bank shall ensure that the name/s of the proposed customers is not appearing in the list of banned entities. In case they find the name of the person in such list, the bank shall (1) not open account of the concerned person (2) seize all documents submitted by him for opening account (3) forward all documents to KYC / AML cell immediately along with their comments and recommendations. The Principal Officer shall put up the facts to the Executive Committee to take a decision of onward reporting as attempted STR to FIU-IND through the Principal Officer of the Bank.
Further, in case of all existing accounts, the AML application shall generate alerts for the names matching with the lists. The branches / AML cell shall scan all the accounts to ensure that no account has been held in the bank by any entities / individuals included in the list or having link to any of them. If AML cell finds that there is any account bearing resemblance with any of the individuals / entities in the list, the Cell shall inform immediately to the Principal Officer the details of account/s. The Principal Officer shall put up the facts to the

Executive Committee to take a decision of onward reporting as attempted STR to FIU-IND and RBI through the Principal Officer of the Bank.

When the bank receives the designated lists from RBI as regard to funds, financial assets or economic resources or related services held in the form of bank accounts, KYC / AML cell at HO shall do the following :-

- Maintain updated designated lists in electronic form and run a check on the given parameters (E.G. Percentage criterion for Name Matching) on a regular basis so that all the Branches can 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.
- In case, the particulars of any of the banks customers match with the particulars of designated individuals / entities, the Branch where the account is maintained shall immediately, **not later than 12 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 KYC / AML Cell at HO.** The Principal Officer shall after approval from the Executive Committee shall report the matter to the Joint Secretary (CTCR), Ministry of Home Affairs (MHA) and shall also convey over telephone within the prescribed time schedule (**at present 24 hours from the time of detection of such account**). The particulars apart from being sent by post shall necessarily be conveyed on e-mail. The Branch should maintain monthly record of the particulars of any of the banks customers match with the particulars of designated individuals / entities. In case such particulars are NIL branch should also maintain the said record on monthly basis.
- The Principal Officer shall also send a copy of the above mentioned communication by post and also by FAX to the UAPA nodal officer of RBI. The particulars apart from being sent by post / FAX shall necessarily be conveyed on e-mail.
- The Principal Officer shall also send a copy of the above mentioned communication to the UAPA nodal officer of the State / Union Territory (appointed by MHA) where the account is held as the case may be and FIU-IND. (List of nodal officers attached)
- In case, the match of any of the customers with the particulars of designated individuals / entities is beyond doubt, the Branches in consultation with KYC / AML cell shall prevent designated person/s from conducting financial transactions. The matter shall be informed to the Principal Officer who shall in turn inform it to the Joint Secretary (CTCR), MHA on Fax and also convey him over telephone. The particulars apart from being sent by post shall necessarily be conveyed on e-mail.
- Branches shall also submit a Suspicious Transaction Report (STR) to the KYC / AML Cell in the matter who shall forward it to the Principal Officer. The Principal Officer shall then after seeking approval from the Executive Committee shall file the report in the prescribed format to FIU-IND covering all transactions carried through or attempted in the accounts.

FIU-INDIA have also given guidelines for effective triggering of Red Flag Indicators (RFI's) with 174 scenarios for implementation. 1 to 94 are system driven scenarios and 95 to 174 are off line scenarios (customers touch point). (Annexure A)

Generation, scrutiny and reporting / clearance of all online VRV alerts will be done at head office level. Generation, scrutiny and clearance of offline VRV and SDN alerts will be done at branch level and reporting of suspicious customers will be done at HO Level. This change will be implemented from 01.04.2022. Record keeping will be done at HO level and branch level for respective alerts.

iv. **Non-profit Organization Transactions Report (NTR)**

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

Confidentiality of information (No Tipping Off)

RBI guidelines require that Banks & their employees shall keep the fact of furnishing of STR strictly confidential, as required under PML Rules. PMLA mandates that the STR related information shall not be revealed to the customers to avoid prejudicing or affecting an investigation, which may be initiated by the law enforcement agencies. The bank shall take utmost precaution to ensure the confidentiality of the information relating to AML. The information shall be made available to the staff on need to know need to basis. The Information Technology Department of the bank shall ensure that necessary controls such as logical access controls, antivirus software etc. are put in place to ensure confidentiality, integrity & need based availability of the information.

5.3.8.5 - Monitoring of Transactions –

Ongoing transaction monitoring is an essential element of effective KYC procedures. Risk can be effectively controlled and reduced only if an understanding of the normal and reasonable activity of the customer is available to identify transactions that fall outside the regular pattern of activity. The extent of monitoring shall depend on the risk sensitivity of the account. Special attention shall be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose.

Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists indicated in Chapter IX of the KYC MD, .

Bank shall put in place an appropriate robust software application to throw alerts when the transactions are inconsistent with risk categorisation and updated profile of customers.

Bank shall prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. The AML application procured by the bank (at present OMNI enterprise by M/S Infra soft) shall generate the alerts as per the rules framed by the bank.

The bank shall generally be guided by the parameters suggested by the Indian Banks Association.

The bank shall implement the parameters as suggested by IBA in a phased manner.

The branches shall also monitor the transactions as per the procedure spelt out in KYC AML Procedures. Branches shall also obtain details of the transactions, over and above specified limits approved by the Bank, from the customers. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer shall attract special attention. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts shall be subject to intensified monitoring. The AML cell shall generate the alerts for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors.
Bank shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorization of customers shall be carried out at a periodicity of not less than once in six months by the AML Cell. The software application shall throw alerts based on the perception of the account for effective monitoring of transactions, identification and reporting of suspicious transactions.
In view of the risks involved in cash intensive businesses, accounts of bullion dealers (including sub-dealers) & Jewellers shall also be categorised by bank as "high risk" requiring enhanced due diligence.

NPCI's official software application Enterprise Fraud Risk Management (EFRM) will be used for all Digital Transaction Online Monitoring i.e. UPI- IMPS- ATM- POS, on 24*7 basis by DB Cell, and if detected any fraud it will be mandatorily reported to RBI through DAKSH Portal. As clearly and specifically mentioned in the training of DAKSH portal given by RBI that DAKSH portal is in development stage, hence every digital fraud should also be mandatorily reported in FMR-I return through XBRL portal, and their updations should be reported in FMR-III return through XBRL portal, in a present prescribed manner and time frame, till further instructions issued by RBI as per the circular issued by RBI on "Central Payments Fraud Information Registry- Migration of Reporting To DAKSH" dated 26/12/2022.

As per ATR dated 15/09/2022, we have submitted to RBI the confidential advisory on detecting Money Mule accounts and Monitoring of Digital transactions, dated 10/08/2022 which mentions the implementation of new alerts for identifying and detection of Money Mule accounts which should be reported to FIU-INDIA as suspected money mule accounts.

Following alerts will also be generated through AML software.
i. Small Accounts with their transactions and periodicity restrictions as per RBI guidelines.
ii. Transactions, if any, from office accounts to checking accounts.
iii. Any transaction that takes place in Sukumar, Chiranjeev, Minor-Guardian accounts after completion of 18 years of age of the account holder.

Following lists are now updated as caution list in AML software for alert generation.
i. Struck off companies as per lists issued by various ROCs.
ii. Banned NGOs. (Quarterly updated list from MHA's FCRA Portal (a- Organizations who's certificate is expired; b-Organizations who's License is cancelled) to be sent to data center for updation in AML Software)
iii. Shell Companies. (Identification of shell companies to be done at branch level at regular intervals and conveyed to HO immediately.)

iv. Attachment orders / enquires / investigation notices received from law enforcement agencies. (SEBI, CBI, ED, Income Tax, Cyber Crime Branch, Court, Police, etc.)
v. Customers reported as deceased and death claim settled.

i. **Reporting Requirements to Financial Intelligence Unit - India –**

Information relating to cash transactions and suspicious transactions and all transactions involving receipts by non-profit organizations of value more than rupees Ten Lakhs or its equivalent in foreign currency are required to be reported to the Director, Financial Intelligence Unit – India (FIU-IND) in respect of transactions referred to in Rule 3. Reserve Bank of India vide Circular No. DBOD AML. BC. 39/14.01.001/2012-13 dated 7th September 2012 has advised all banks to introduce single XML reporting format.

REs shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.
Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the REs for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.
The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by REs which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data.
While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. Bank shall not put any restriction on operations in the accounts where an STR has been filed. Bank shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.
Robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

SOP for VRV and SDN alerts generation and clearance: (As per FIU-INDIA guidelines Dt. 28/09/2020 - Implementation of 174 alerts.)
Implementation of newly introduced 174 Red Flag Indicators (RFIs)
Ref – FIU-IND circular dated 28/09/2020. (Guidelines for effective detection and reporting of suspicious transactions) and 11/05/2021 (Guidelines for reporting STR in which suspicious credits and debits through UPI are reported)

The above letter gives direction to implement new 174 RFIs (alerts) for generation of STRs for submission to FIU-IND. It contains
Annexure 1 – List 1 – System driven scenarios (1-94 online alerts)
Annexure 2 – List 2 – Offline scenarios (95-174 – customer touch point alerts)
Annexure 3 – Monitoring scenario, thresholds setting and tuning (guideline)
Annexure 4 – Model Template for STR and Guideline for filing STRs.
Annexure 4- Model Template for STR (GOS Part) and Guideline for filing STRs - Clarification
Offline scenarios are already implemented from 30.09.2021. Outreach meeting on this subject was jointly held by FIU-IND and RBI on 20/07/2021 and was minitize wherein the timeline for implementing all the scenarios was set as 30.09.2021.

For offline scenarios register to be newly prepared and maintained namely "Offline AML Alerts" at branch level for every reported suspicious transaction.

Entire guideline with all annexures i.e. all online & offline RFIs with their threshold limits were discussed, finalized and sanctioned in various KYC AML Committee meetings.

SOP for the above is also sanctioned by Hon. Chief Executive Officer vide note dated 14.01.2022 which is duly approved by Hon Board of Directors meeting dated 31.01.2022 and is to be considered as a part of this policy. (Annexure)

All available SDN lists (UN, OFAC) on the United Nations website, Banned organizations list from MHA website and all such other lists as guided by RBI to be downloaded and sent to data center for uploading them in our AML Software minimum twice in a month including any updation (addition / deletion) according to implementation of sec 51(A) of UAPA, 1697 is received from RBI, should be sent to data center for updation on 'as and when' received basis.

Following alerts will also be generated through AML software.
i. Small Accounts with their transactions and periodicity restrictions as per RBI guidelines.
ii. Transactions, if any, from office accounts to checking accounts.
iii. Any transaction that takes place in Sukumar, Chiranjeev, Minor-Guardian accounts after completion of 18 years of age of the account holder.

Following lists are now updated as caution list in AML software for alert generation.
i. Struck off companies.
ii. Banned NGOs. (Quarterly updated list from MHA's FCRA Portal (a- Organizations who's certificate is expired; b-Organizations who's License is cancelled) to be sent to data center for updation in AML Software)
iii. Shell Companies. (Identification of shell companies to be done at branch level at regular intervals and conveyed to HO immediately.)
iv. Attachment orders / enquires / investigation notices received from law enforcement agencies. (SEBI, CBI, ED, Income Tax, Cyber Crime Branch, Court, Police, etc.)

Requirements/obligations under International Agreements Communications from International Agencies –

REs 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 UAPA notification dated 55(Annex II of this Master Direction). February 2, 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.

5.3.9 - Training –

Sec 70. (Of updated MD on KYC – 10.05.2021) - Hiring of Employees and Employee training and RBI letter dated 20/10/2021-

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

(ii) On-going employee training programme shall be put in place so that the members of staff are adequately trained in 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 RE, regulation and related issues shall be ensured.

Training with respect of the above subject to be provided to all the staff of the bank (even at branch level) via online / offline modes. Some of the points that need to be covered under these training are enlisted in RBI letter dated 20/10/2021.

Also, bank should provide information regarding various aspects and importance of KYC / AML areas and its compliance to our customers through various modes like, sms, mail, mobile app, website, and small videos on branch TV set, small posters at branch and ATM premises, etc.

a. Making of employees aware of the findings of internal ML/TF risk assessment report.

b. Enrich staff knowledge using certification programs.

c. Sensitization of staff on KYC/AML/CFT matters including exposure to certain financial crime scenarios and case studies.

d. Explain program on FATF Mutual evaluation process and its significance.

e. Basic information about FATF recommendations on risk based approach, internal ML/TF risk assessment, CDD requirements, beneficial owner's identifications and sanctions list screenings, etc.

f. Knowledge about RFIs may be raised by the dealing staff (human intelligence)

g. Updation of training material with amendments and instruction / advisory issued by RBI, FIU-IND, IBA, etc.
h. Information about high risk customers and EDD of such customers.
i. Procedure of identification of BO for LE customers.
j. Requirement of risk categorisation.
k. Knowledge of modus operandi adopted for defrauding public through use of Money Mule accounts.

Cluster wise training in consort with online and offline training programmes will be arranged for all branches as and when required.

Trainings for staff dealing in KYC/AML/CFT matters should include elements of open communication, high-integrity and proper understanding of subject matter.

5.3.10 - Frauds- Classification and Reporting (With reference to the RBI Master direction dated 01 July 2015)

Incidence of frauds, dacoities, robberies, etc., in banks is a matter of concern.
While the primary responsibility for preventing frauds lies with banks themselves, the Reserve Bank of India (RBI) has been advising banks from time to time about the major fraud prone areas and the safeguards necessary for prevention of frauds. RBI has also been circulating to banks, the details of frauds of an ingenious nature not reported earlier so that banks could introduce necessary safeguards by way of appropriate procedures and internal checks. To facilitate this ongoing process, it is essential that banks report to the Reserve Bank full information about frauds and the follow-up action taken thereon. Banks may, therefore, adopt the reporting system for frauds as prescribed in the following paragraphs.
It has been observed that frauds are, at times, detected in banks long after their perpetration. The fraud reports are also submitted to the RBI, many a time, with considerable delay and without the required information. On certain occasions, the RBI comes to know about frauds involving large amounts only through press reports. Banks should, therefore, ensure that the reporting system is suitably streamlined so that frauds are reported without any delay. Banks must fix staff accountability in respect of delays in reporting fraud cases to the RBI.
Delay in reporting of frauds and the consequent delay in alerting other banks about the modus operandi and issue of caution advices against unscrupulous borrowers could result in similar frauds being perpetrated elsewhere. Banks may, therefore, strictly adhere to the timeframe fixed in this circular for reporting fraud cases to RBI failing which banks would be liable for penal action as prescribed under Section 47(A) of the Banking Regulation Act, 1949 (As applicable to Co-operative Societies).

- A separate committee named "Fraud Monitoring Committee" was established for taking care of every aspect relating to fraud right from investigating to reporting as approved in the capacity of Hon. CEO sir vide sanction note no. 277 dated 08/03/2023.

- The Bank has specifically nominated a Principal Officer, who shall be responsible for submitting all the returns referred to in this circular.

CLASSIFICATION OF FRAUDS

In order to have uniformity in reporting, frauds have been classified as under, based mainly on the provisions of the Indian Penal Code:

i) Misappropriation and criminal breach of trust.
ii) Fraudulent encashment through forged instruments, manipulation of books of account or through fictitious accounts and conversion of property.
iii) Unauthorised credit facilities extended for reward or for illegal gratification.
iv) Negligence and cash shortages.
v) Cheating and forgery.
vi) Irregularities in foreign exchange transactions.
vii) Any other type of fraud not coming under the specific heads as above.

Cases of 'negligence and cash shortages' and 'irregularities in foreign exchange transactions' referred to in item (d) & (f) above are to be reported as fraud if the intention to cheat/defraud is suspected/ proved. However, the following cases where fraudulent intention is not suspected/proved at the time of detection will be treated as fraud and reported accordingly:

- cases of cash shortages of more than '10,000' and
- cases of cash shortages of more than '5,000' if detected by management/auditor/inspecting officer and not reported on the day of occurrence by the persons handling cash.

To ensure uniformity and to avoid duplication, frauds involving forged instruments may be reported only by the paying banker and not by the collecting banker.

However, in the case of collection of an instrument which is genuine but the amount is collected fraudulently by a person who is not the true owner, the collecting bank, which is defrauded, will have to file fraud report with the RBI.

In case of collection of instrument where the amount has been credited and withdrawn before realisation and subsequently the instrument is found to be fake/forged and returned by the paying bank, it is the collecting bank who has to file FMR-1 with the RBI as they are at loss by parting the amount before realisation of the instrument.

Encashment of altered / fake cheques involving two or more branches of same bank

In case of collection of altered/fake cheque involving two or more branches of the same bank, the branch where the altered/fake cheque has been encashed, should report the fraud to Head Office of the bank. Thereafter, Head Office of the bank will file the fraud report with RBI.

In the event of an altered/fake cheque having been paid/encashed involving two or more branches of a bank under Core Banking Solution (CBS), there could be a possibility of dispute/difference of opinion as to whether the branch where the drawer of the cheque maintains the account or the branch where the encashment has taken place should report the matter to the Head Office of the bank. In such cases also the branch which has released

the payment against an altered / fake cheque should report the fraud to the Head Office. Thereafter, Head Office of the bank will file the fraud report with RBI.

REPORTING OF FRAUDS TO RESERVE BANK OF INDIA

Frauds involving amounts of less than '1.00 lakh'

The cases of individual frauds involving amounts of less than '1.00 lakh are not to be reported individually to the RBI. Statistical data in respect of such frauds should, however, be submitted to RBI in a quarterly statement as detailed in Para below.

Frauds involving amounts of 1.00 lakh and above but less than 25 lac

The cases of individual frauds involving amounts of 1.00 lakh and above but less than 25.00 lakh should be reported to the Regional Office of Department of Cooperative Bank Supervision of Reserve Bank of India, under whose jurisdiction the Head Office of the bank falls, in the format given in FMR-1, within three weeks from the date of detection.

Frauds involving amounts of ` 25.00 lakh and above

The cases of individual frauds involving amounts of Rs. 25.00 lakh and above should be reported to Central Frauds Monitoring Cell, Department of Banking Supervision, Reserve Bank of India, 10/3/8, Nruputhunga Road, P.B.No. 5467, Bengaluru- 560 001 in the format given in FMR-1, within three weeks from the date of detection. Separate FMR-1 should be furnished in respect of each, case without clubbing. A copy of FMR-1 should also be submitted to the Regional Office of Department of Cooperative Bank Supervision of Reserve Bank of India under whose jurisdiction the Head Office of the bank falls.

In addition to the requirement given above, as per RBI circular dated 19.05.2016, regarding changes in monitoring and reporting mechanism of frauds, bank may report the fraud of Rs. 1.00 crore and above by means of D.O. letter addressed to the Principal Chief General Manager of the Department of Banking Supervision, Reserve Bank of India, Central Office, within a week of such fraud coming to the notice of the bank's Head Office. The letter may contain brief particulars of the fraud such as amount involved, nature of fraud, modus operandi in brief, name of the branch/office, names of parties involved (if they are proprietorship/partnership concerns or private limited companies, the names of proprietors, partners and directors), names of officials involved and whether a complaint has been lodged with the Police. A copy of the D.O. letter should also be endorsed to the Regional Office of Department of Cooperative Bank Supervision of Reserve Bank of India under whose jurisdiction the bank's branch, where the fraud has been perpetrated, is functioning.

As mentioned in the RBI letter to all Primary Urban Co-operative Banks dated 26.07.2021, hard copy for reporting of frauds is discontinued and frauds shall be reported only through online portal of RBI (XBRL)

Frauds committed by unscrupulous borrowers

It is observed that a large number of frauds are committed by unscrupulous borrowers including companies, partnership firms/proprietary concerns and/or their directors/partners by various methods including the following:

(i) Fraudulent discount of instruments or kite flying in clearing effects.

(ii) Fraudulent removal of pledged stocks/disposing of hypothecated stocks without the bank's knowledge/inflating the value of stocks in the stock statement and drawing excess bank finance.
(iii) Diversion of funds, lack of interest or criminal neglect on the part of borrowers, partners etc. in adhering to financial discipline and managerial failure with malafide intent leading to the unit becoming sick and laxity in effective supervision over the operations in borrowal accounts on the part of the bank functionaries rendering the advance difficult for recovery and resulting in financial loss to the bank.

In respect of frauds in borrowal accounts additional information as prescribed under Part B of FMR – 1 should also be furnished.

All the branches and departments of the bank have to mandatorily report any nature / type of fraud (as mentioned above) involving any amount detected in their branch / department on the same day to AML Cell for further reporting to RBI. As a prudent policy of the bank, after such reporting of frauds is done by the branches / departments, every fraud of whatsoever amount will be reported to RBI by AML Cell within the stipulated time.

FMR Certificate - All the irregularities, fraud cases, etc. detected in the bank for the entire month is to be reported to The Reserve Bank of India (Central Fraud Monitoring Cell, Bengaluru and Department of Co-Operative Bank Supervision, BKC, Mumbai) within 7 days of the succeeding month. Even if there are no irregularities or frauds detected during the month, a NIL report is to be sent within the due date.
FMR-1 certificate is submitted through email to dbscofmrc@rbi.org.in, mrooss1@rbi.org.in and oss@rbi.org.in & hard copy through speed post is sent to Principal CGM, Central Fraud Monitoring Cell, DBS, RBI, Bengaluru and CGM, RBI Mumbai Regional Office, BKC, Bandra East, Mumbai.

Providing information and details to AML Cell relating to any incidence, whether fraud or irregularity, occurred in any branch / department of the bank, should be conveyed immediately (on as and when occurs basis). Failing which there may be a monetary penalty imposed on the bank for late reporting by RBI, and it will be the sole responsibility for the concerned branch / department.

Cases of attempted fraud. - The practice of reporting attempted fraud, where likely loss would have been Rs.25 lakhs or more to Fraud Monitoring Cell, Department of Banking Supervision, Reserve Bank of India, Central Office has been discontinued in terms of circular dated March 08, 2013. However, the bank should continue to place the individual cases of attempted fraud involving Rs.25 lakhs or more before the Audit Committee of its Board. The report containing attempted frauds which is to be placed before the Audit Committee of the Board should cover the following viz.

* The modus of operandi of attempted fraud
* How the attempt did not materialize into a fraud or how the attempt failed / or was foiled.
* The measures taken by the bank to strengthen the existing systems and controls.
* New systems and controls put in place in the area where fraud was attempted,

* In addition, yearly consolidated review of such cases detected during the year containing information such as area of operations where such attempts were made, effectiveness of new process and procedures put in place during the year, trend of such cases during the last three years, need for further change in process and procedures, if any, etc. as on March 31 every year may be placed before the Audit Committee of the Board starting from the year ending March 31, 2013 within three months from the end of the relative year.

All the branches and departments of the bank have to mandatorily report any nature / type of attempted fraud (as mentioned above) involving any amount detected in their branch / department on the same day to AML Cell for further reporting to Hon. Audit Committee of the Board (ACB). As a prudent policy of the bank, after such reporting of frauds is done by the branches / departments, every attempted fraud of whatsoever amount will be reported to ACB by AML Cell through monthly reporting.

Disclosure of Fraud accounts –

As per RBI Guidelines – Master directions on financial statements, presentation and disclosers, Banks shall make disclose details on the number and amount of frauds as well as the provisioning thereon as per template given below (To be included in disclosure in financial statements – notes to accounts)

(Rs. In Crores)

	Current year	Previous year
Number of frauds reported		
Amount involved in fraud		
Amount of provision made for such frauds		
Amount of Unamortized provision debited from 'other reserves' as at the end of the year		

Provisioning Pertaining to Fraud Accounts

It has been decided to prescribe a uniform provisioning norm in respect of all cases of fraud, as under:

i. The entire amount due to the bank (irrespective of the quantum of security held against such assets), or for which the bank is liable (including in case of deposit accounts), is to be provided for over a period not exceeding four quarters commencing with the quarter in which the fraud has been detected;

However, where there has been delay, beyond the prescribed period, in reporting the fraud to the Reserve Bank, the entire provisioning is required to be made at once. In addition, Reserve Bank of India may also initiate appropriate supervisory action where there has been a delay by the bank in reporting a fraud, or provisioning there against.

RETURNS –

Report on Frauds Outstanding (FMR-2) - FMR-2 Report on Fraud outstanding is discontinued as per The Reserve Bank of India letter dated 27/08/2018 and email dated 30.08.2018 (email received from UBD, MRO Return)

Progress Report on Frauds (FMR-3)

Banks should furnish case-wise quarterly progress reports on frauds involving ` 1.00 lakh and above in the format given in FMR–3 to the Regional Office of Department of Cooperative Bank Supervision of Reserve Bank of India under whose jurisdiction the bank's Head Office is situated, within 15 days of the end of the quarter to which it relates.

In case of frauds where there are no developments during a quarter, a list of such cases with brief description including name of branch and date of reporting may be furnished in Part – B of FMR – 3.

If there are no fraud cases involving 1.00 lakh and above outstanding, banks may submit a nil report.

As mentioned in the RBI letter to all Primary Urban Co-operative Banks dated 26.07.2021, hard copy for reporting of frauds is discontinued and frauds shall be reported only through online portal of RBI (XBRL). Taking this into consideration and also the existing online format of FMR-3 on XBRL portal, list of cases with brief description and also NIL reporting is not available.

Also, as conveyed in the joint training conducted by RBI and FIU-IND, FMR-3 was converted to FUA (Fraud Update Application) and reporting timeline was changed to 'As and when updated'.

REPORTING TO THE BOARD

AML Department should ensure that all frauds of 1.00 lakh and above are reported to their Boards promptly on their detection.

Such reports should, among other things, take note of the failure on the part of the concerned branch officials and controlling authorities, and consider initiation of appropriate action against the officials responsible for the fraud.

Quarterly Review of Frauds

Information relating to frauds for the quarters ending June, September and December may be placed before the Audit Committee of the Board of Directors during the month following the quarter, to which it pertains, irrespective of whether or not these are required to be placed before the Board / Management Committee in terms of the Calendar of Reviews prescribed by the Reserve Bank of India.

A separate review for the quarter ending March is not required in view of the Annual Review for the year ending March prescribed below. The review for the year ended March may be placed before the Board before the end of next quarter. i.e. for the quarter ended June 30.

Special Committee of Board for Monitoring High Value Frauds

As delay in various aspects of frauds like detection, reporting to regulatory and enforcement agencies and action against the perpetrators of the frauds had been causing concern, the need was felt for paying focused attention on monitoring of frauds at the highest level and it was suggested to constitute a subcommittee of the Board which would be exclusively dedicated to the monitoring of fraud cases. It has therefore been decided that Boards of banks should constitute a Special Committee for monitoring and following up cases of frauds involving amounts of Rs.1 crore and above exclusively, while ACB may continue to monitor all the cases of frauds in general.

(i) The broad guidelines regarding constitution and functions of the Special Committee of the Board are follows:

a) Constitution of the Special Committee
The Special Committee may be constituted with five members of the Board of Directors including Chairman, two members from ACB, and two other members from the Board.

b) Functions of Special Committee
The major functions of the Special Committee would be to monitor and review all the frauds of Rs.1 crore and above so as to;

- Identify the systemic lacunae if any that facilitated perpetration of the fraud and put in place measures to plug the same;
- Identify the reasons for delay in detection, if any, reporting to top management of the bank and RBI;
- Monitor progress of CBI / Police Investigation, and recovery position and;
- Ensure that staff accountability is examined at all levels in all the cases of frauds and staff side action, if required, is completed quickly without loss of time.
- Review the efficacy of the remedial action taken to prevent recurrence of frauds, such as strengthening of internal controls.
- Put in place other measures as may be considered relevant to strengthen preventive measures against frauds.

c) Meetings
The periodicity of the meetings of the Special Committee may be decided according to the number of cases involved. However, the Committee should meet and review as and when a fraud involving an amount of Rs.1 crore and above comes to light.

d) Review of the functioning of the Special Committee
The functioning of the Special Committee of the Board may be reviewed on a half yearly basis and the reviews where applicable may be put up to the Board of Directors.

Annual Review of Frauds

Banks should conduct an annual review of the frauds and place a note before the Board of Directors for information.
The main aspects which may be taken into account while making such a review may include the following:

i. Whether the systems in the bank are adequate to detect frauds, once they have taken place, within the shortest possible time.
ii. Whether frauds are examined from staff angle and, wherever necessary, the staff side action is taken without undue delay.
iii. Whether deterrent punishment is meted out, wherever warranted, to the persons found responsible without undue delay.
iv. Whether frauds have taken place because of laxity in following the systems and procedures or loopholes in the system and, if so, whether effective action has been taken to ensure that the systems and procedures are scrupulously followed by the staff concerned or the loopholes are plugged.
v. Whether frauds are reported to the local Police for investigation.

The annual reviews should also, among other things, include the following details:

i. Total number of frauds detected during the year and the amount involved as compared to the previous two years.
ii. Analysis of frauds according to different categories detailed above.
iii. Modus operandi of major frauds reported during the year along with their present position.
iv. Detailed analysis of frauds of 1.00 lakh and above.
v. Estimated loss to the bank during the year on account of frauds, amount recovered and provisions made.
vi. Number of cases (with amounts) where staff are involved and the action taken against staff.
vii. Time taken to detect frauds (number of cases detected within three months, six months, one year, more than one year of their taking place).
viii. Position with regard to frauds reported to the Police.
ix. Number of frauds where final action has been taken by the bank and cases disposed-off.
x. Preventive/punitive steps taken by the bank during the year to reduce/minimise the incidence of frauds. Whether systems and procedures have been examined to ensure that weaknesses are addressed.

GUIDELINES FOR REPORTING OF FRAUDS TO POLICE

Banks should follow the following guidelines for reporting of frauds such as unauthorised credit facilities extended by the bank for illegal gratification, negligence and cash shortages, cheating, forgery, etc. to the State Police authorities:

i. In dealing with cases of fraud/embezzlement, banks should not merely be motivated by the necessity of recovering expeditiously the amount involved, but should also be motivated by public interest and the need for ensuring that the guilty persons do not go unpunished.
ii. Therefore, as a general rule, the following cases should invariably be referred to the State Police:

a. Cases of fraud involving an amount of 1.00 lakh and above, committed by outsiders on their own and/or with the connivance of bank staff/officers.
b. Cases of fraud committed by bank employees, when it involves banks' funds exceeding 10,000

Filing of Police complaint in case of fraudulent encashment of DDs/TTs/Pay Orders/Cheques/Dividend Warrants, etc.

In case of frauds involving forged instruments, the paying banker has to file the police complaint (FIR) and not the collecting banker.

However, in case of collection of instrument which is genuine but the amount collected fraudulently by a person who is not the owner, the collecting bank which is defrauded has to file a police complaint (FIR).

In case of collection of instruments where the amount has been credited before realisation and subsequently the instrument is found to be fake/forged and returned by the paying bank, it is the collecting bank who has to file a police complaint as they are at loss by paying the amount before realisation of the instrument.

In cases of collection of altered/fake cheque involving two or more branches of the same bank, the branch where the altered/fake instrument has been encashed, should file a Police complaint (FIR).

In the event of an altered / fake cheque having been paid /encashed involving two or more branches of a bank under CBS, the branch which has released the payment against a fraudulent withdrawal, should file a Police complaint.

CLOSURE OF FRAUD CASES

Banks will report to the concerned Regional Office of Department of Cooperative Bank Supervision of Reserve Bank of India under whose jurisdiction the Head Office of the bank falls, the details of the fraud cases closed along with reasons for the closure where no further action was called for. Fraud cases closed during the quarter are required to be reported in quarterly return FMR-2.

Banks should report only such cases of frauds as closed where the actions as stipulated below are complete.

a. The fraud cases pending with Police/Courts are finally disposed.
b. The examination of staff accountability has been completed.
c. The amount of fraud has been recovered or written off.
d. Insurance claim, wherever applicable, has been settled.
e. The bank has reviewed the systems and procedures, identified the causative factors and plugged the lacunae and the fact of which has been certified by the Board. Banks should also pursue vigorously with the Police/Court for final disposal of the pending cases especially where the banks have completed staff side action.

Reporting Cases of Theft, Burglary, Dacoity and Bank Robberies (FMR -4)

Banks should arrange to report by fax / e-mail instances of thefts, burglaries dacoities and robberies to the following authorities immediately on their occurrence.

i. The Principal Chief General Manager, Reserve Bank of India, Department of Cooperative Bank Supervision, Central Office, Garment House, Worli, Mumbai 400 018.

ii. Regional Office of Reserve Bank of India, Department of Cooperative Bank Supervision of the state in which the theft/burglary/dacoity/robbery has taken place to enable the Regional Office to take up the issues with the concerned authorities regarding security arrangements in the affected branch/es (endorsement).
The report should include details of modus operandi and other information as at columns 1 to 11 of FMR – 4.
Banks should also submit to concerned Regional Office of the Reserve Bank of India, Department of Cooperative Bank Supervision under whose jurisdiction the bank's Head Office is situated a quarterly consolidated statement in the format given in FMR – 4 covering all cases pertaining to the quarter. This may be submitted within 15 days of the end of the quarter to which it relates.
Banks which do not have any instances of theft, burglary, dacoity and/ or robbery to report during the quarter may submit a nil report.
All the instances of theft, burglary, dacoity and/ or robbery are to be reported to the Hon. Board of Directors in the forthcoming monthly meeting after which FMR-4 is submitted to RBI.

As per RBI circular dated 26.07.2021, urban co-operative banks have been instructed to discontinue submission of returns in hard copy and only use XBRL portal for return submission. (i.e. FMR-1, FMR-3 & FMR-4)

In view of the recommendations made by the Damodaran Committee (dated 03.08.2011 – Chapter 2, sec 8 (23) – Information on fraudulent accounts), information on fraudulent accounts among banks should be shared with other banks to prevent repeated occurrences of such frauds. In light of this, if any incident occurs, such information should be conveyed to IBA on quarterly basis. No NIL report to be submitted, vice-versa, information on frauds received from IBA, is to circulated to all staff members as precautionary measures.

5.3.11 - SOP for Risk Based Approach to KYC-AML Quarterly Supervision Data & Yearly Documents -

Ref:- RBI Letter Dos.CO.KYC.AML./518/11.01.069/2021-22 dated 08/04/2021.

Mutual Evaluation of all the member countries will be done by FATF, India's mutual evaluation is due to be made in the year 2022-23. National Risk Assessment would be done from FATF and risk rating will be given to the country accordingly. Such risk rating has high importance in the international market.

For such assessment, exhaustive data templates are to be submitted to RBI on quarterly basis from which RBI will give gradation / risk rating to the respective bank. So submitting accurate and integrated data is binding on the bank. Our bank is among top 10 largest urban co-operative bank in the country. So, incorrect data submission on such a large scale will have adverse effect on the mutual evaluation of the country. RBI has specially instructed large

banks to take extra precautions while submitting the data. Hence, incorrect data submission will be taken adversely by RBI.

The above letter gives direction to submit quarterly data in 38 templates (charts) after 30 days from the quarter end date along with 17 yearly documents within 2.5 months from year-end date.

Timeline for submitting data for December 2020 quarter along with 4 preceding quarters i.e. Dec 19, March 20, June 20 and Sept 20 should be submitted by 31.05.2021. Data for March 2021 quarter with yearly documents to be submitted by 15.06.2021.

From above mentioned 38 templates, 20 templates will be prepared and shared with us by Infrasoft Tech company and data for 18 templates and 17 yearly documents is to be generated in-house i.e. by the bank (data to be collected from all concerned departments of the bank on quarterly basis).

For country-wise risk classification, bank should refer the country-wise risk classification as published by FATF from time to time.

Nodal Officer of the bank for all the above process is to be appointed. General Manager, KYC AML Cell will act as the Nodal Officer for the above process and is already conveyed to RBI.

The detailed description and information of each template and yearly document which will be developed in-house, i.e. 18 templates and 17 documents is sanctioned by Hon. Chief Executive Officer vide note dated 14.01.2022 which is duly approved by Hon. Board of Directors meeting dated 31.01.2022 and is to be considered as a part of this policy. (Annexure B)

Entire guideline with all annexures i.e. 38 templates and 17 documents, with their parameters and required information were discussed, finalized and sanctioned in KYC AML Committee meetings.

Following reports / returns are to be submitted to Hon BOD/ ACB and senior management covering KYC aml areas (details regarding this is also mentioned in Annexure A)-

i. Monthly Review Report a. For KYC, AML (Information regarding Re-KYC, CKYC, CCR, CTR, STR, NTR, NCRB, Vigilance, Beneficial Owner compliance, etc.); b. Regarding Frauds cases (Information related to FMR-1, FUA and FMR-4, attempt to fraud cases, irregular activities, etc.)
ii. Detailed quarterly review report for all existing fraud cases.
iii. Half yearly Risk assessment report.
iv. Suspicious Transaction Report submitted to senior management after every Committee meeting.

Risk Based Approach Supervision Data are templates and documents with exhaustive data and is to be quarterly submitted to RBI. For this submission, customers' data should be

collected correctly and completely and filled in the system accordingly for proper report generation.

Providing all the data required from various departments for submission of above templates and standard documents within prescribed timeline will be the sole responsibility of the concerned department.

All foreign transactions should be identified and reported separately, it should be divided into two parts i.e. trade based transactions and non-trade based transactions. All forex transactions related to trade or business are to be reported under trade based transactions, and all other are to be reported s non-trade based transactions. Also, passing of transaction in Omni3.0 system should be done in separate newly prepared batches i.e.

i. Inward Forex Transactions – Trade based (Fx-ITB)
ii. Inward Forex Transactions – Non-Trade based (Fx-INTB)
iii. Outward Forex Transactions – Trade based (Fx-OTB)
iv. Outward Forex Transactions – Non-Trade based (Fx-ONTB)

Issuing of Letter of Credit (LCs) and Bank Guarantees (BGs) are also to be divided as Foreign LC / BG (trade based and non-trade based) and Inland LC / BG (trade based and non-trade based). This is also to be reported as per newly introduced GL Heads as under.

i. Inland BG – Trade based	i. Inland LC – Trade based
ii. Inland BG – Non-Trade based	ii. Inland LC – Non-Trade based
iii. Foreign BG – Trade based	iii. Foreign LC – Trade based
iv. Foreign BG – Non-Trade based	iv. Foreign LC – Non-Trade based

5.3.12 - Provisions as per Unlawful Activities (Prevention) Act, 1967

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

(a) Bank 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:

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

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

Bank shall also ensure to refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as

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

Henceforth downloading and uploading sanction lists will be done on weekly basis and additionally as and when required according to reported by Regulator Entity, in our AML software.

(b) 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 (MHA) as required under UAPA notification dated 105February 2, 2021 (Annex II of this Master Direction).

The Additional Secretary (CTCR), Ministry of Home Affairs would be the Central [designated] Nodal Officer for the UAPA [Telephone Number: 011-23092456, 011-230923465 (Fax), email address: jsctcr-mha@gov.in].

(c) Freezing of Assets under Section 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated 106February 2, 2021 (Annex II of this Master Direction) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA.

A. Freezing of Assets under Section 51A of UAPA, 1967

Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) reads as under:-

"51A. For the prevention of, and for coping with terrorist activities, the Central Government shall have power to —

i) 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;

ii) 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;

iii) prevent the entry into or the transit through India of individuals listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism".

The Unlawful Activities (Prevention) Act, 1967 defines "Order" as under:-

"Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order. 2007, as may be amended from time to time.

In order to expeditiously and effectively implement the provisions of Section 51A, a procedure was outlined vide this Ministry Order No. 17015/10/2002-IS-VI dated 27.08.2009. After the reorganization of the Divisions in Ministry of Home Affairs, the administration of Unlawful Activities (Prevention) Act, 1967 and the work relating to countering of terror financing has been allocated to the CTCR Division. The order dated 27.8.2009 is accordingly modified as under:

Appointment and communication of details of UAPA Nodal Officers

As regards appointment and communication of details of UAPA Nodal Officers-

(i) The UAPA Nodal Officer for CTCR Division would be the Joint Secretary (CTCR), Ministry of Home Affairs. His contact details are 011-23092736 (Tel), 011-23092569 (Fax) and jsctcr-mha@gov.in (e-mail id).

(ii) The Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, FIU-IND; and RBI, SEBI, IRDA (hereinafter referred to as Regulators) shall appoint a UAPA Nodal Officer and communicate the name and contact details to the CTCR Division in MHA.

(iii) The States and UTs should appoint a UAPA Nodal Officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the CTCR Division in MHA.

(iv) The CTCR Division in MHA would maintain the consolidated list of all UAPA Nodal Officers and forward the list to all other UAPA Nodal Officers.

(v) The RBI, SEBI, IRDA should forward the consolidated list of UAPA Nodal Officers. to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively.

(vi) The consolidated list of the UAPA Nodal Officers should be circulated by the Nodal Officer of CTCR Division of MHA in July every year and on every change. Joint Secretary (CTCR) being the Nodal Officer of CTCR Division of MHA, shall cause the amended list of UAPA Noda! Officers to be circulated to the Nodal Officers of Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, RBI, SEBI, IRDA and FIU-IND.

Communication of the list of designated individuals/entities

As regards communication of the list of designated individuals/entities-

(i) The Ministry of External Affairs shall update the list of individuals and entities subject to UN sanction measures on a regular basis. On any revision, the Ministry of External Affairs would electronically forward this list to the Nodal Officers in Regulators, FIU-IND, CTCR Division and Foreigners Division in MHA,

(ii) The Regulators would forward the list mentioned in (i) above (referred to as designated lists) to the banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies respectively.

(iii) The CTCR Division of MHA would forward the designated lists to the UAPA Nodal Officer of all States and UTs.

(iv) The Foreigners Division of MHA would forward the designated lists to the immigration authorities and security agencies.

- On receipt of, the particulars as mentioned above, (Counter terrorism and counter radicalization) CTCR Division of MHA shall 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 bank are the ones listed as designated individuals / entities and the funds, financial assets or economic resources or related services reported by the bank are held by the designated individuals / entities. This verification shall be completed within a period not exceeding five 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 51 A of the UAPA shall be issued within 24 hours of such verification and conveyed electronically to the bank / the Branch concerned under intimation to the RBI and FIU-IND.

- The Order shall take place without prior notice to the designated individuals / entities.
- On receipt of an order from competent authority conveyed electronically to the bank / the Branch concerned, to freeze the assets of an individual or entity under Section 51 A of the UAPA the bank/branch shall act on the same without delay.
- The procedure laid down in the UAPA Order dated February 2, 2021 (Annex II of this Master Direction) 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. (Annexure C)

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

(i) 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.

(ii) 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 Section 55 a & b do not preclude REs from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

(iii) 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.

C. Secrecy Obligations and Sharing of Information (Sec 55 of KYC MD):

(i) Banks shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.

(ii) 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.

(iii) 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.

(iv) The exceptions to the said rule shall be as under:

a. Where disclosure is under compulsion of law

b. Where there is a duty to the public to disclose,

c. the interest of bank requires disclosure and

d. Where the disclosure is made with the express or implied consent of the customer.

D. Regarding funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc.

The Financial Regulators will issue necessary guidelines to banks, stock exchanges/depositories, intermediaries regulated by the SEBI and insurance companies requiring them -

(i) To maintain updated designated lists in electronic form and run a check on the given parameters on a daily basis to verify whether individuals or entities listed in the Schedule to the Order, hereinafter, 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, stocks, Insurance policies etc., with them.

(ii) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the banks, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies shall immediately inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc., held by such customer on their books to the Central [designated] Nodal Officer for the UAPA, at Fax No.011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: jsctcr-mha@gov.in.

(iii) The banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall also send a copy of the communication mentioned in 5.1 (ii) above to the UAPA Nodal Officer of the State/UT where the account is held and to Regulators and FIU-IND, as the case may be, without delay.

(iv) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall prevent such designated persons from conducting financial transactions, under intimation to the Central [designated] Nodal Officer for the UAPA at Fax No.011-23092551 and also convey over telephone No.011-23092548. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsctcr-mha@gov.in, without delay.

(v) The banks, stock exchanges/depositories, intermediaries regulated by SEBI, and insurance companies shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts, covered under Paragraph 5.1(ii) above, carried through or attempted as per the prescribed format.

On receipt of the particulars, as referred to in Paragraph 5 (i) above, the Central [designated] Nodal Officer for the UAPA 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, stock exchanges/depositories, intermediaries and insurance companies are the ones listed as designated individuals/ entities and the funds, financial assets or economic resources or related services, reported by banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies are held by the designated individuals/entities. This verification would be completed expeditiously from the date of receipt of such particulars.

In case, the results of the verification indicate that the properties are owned by or are held for the benefit of the designated individuals/entities, an orders to freeze these

assets under Section 51A of the UAPA would be issued by the Central [designated] nodal officer for the UAPA without delay and conveyed electronically to the concerned bank branch, depository and insurance company under intimation to respective Regulators and FIU-IND. The Central [designated] nodal officer for the UAPA shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and all UAPA nodal officers in the country, so that any individual or entity may be prohibited from making any funds, financial assets or economic resources or related services available for the benefit of the designated individuals/ entities or any other person engaged in or suspected to be engaged in terrorism. The Central [designated] Nodal Officer for the UAPA shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967.

The order shall be issued without prior notice to the designated individual/entity.

E. Regarding financial assets or economic resources of the nature of immovable properties:

The Central [designated] Nodal Officer for the UAPA shall electronically forward the designated list to the UAPA Nodal Officers of all States and UTs with request to have the names of the designated individuals/entities, on the given parameters, verified from the records of the office of the Registrar performing the work of registration of immovable properties in their respective jurisdiction, without delay.

In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property and if any match with the designated individuals/entities is found, the UAPA Nodal Officer of the State/UT would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources of the nature of immovable property to the Central [designated] Nodal Officer for the UAPA without delay at Fax No. 011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post would necessarily be conveyed on email id: jsctcr-mha@gov.in.

The UAPA Nodal Officer of the State/UT may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent by the Registrar performing the work of registering immovable properties are indeed of these designated individuals/entities. This verification shall be completed without delay and shall be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual/entity to the Central [designated] Nodal Officer for the UAPA at the given Fax, telephone numbers and also on the email id.

The Central [designated] Nodal Officer for the UAPA may also have the verification conducted by the Central Agencies. This verification would be completed expeditiously.

In case, the results of the verification indicates that the particulars match with those of designated individuals/entities, an order under Section 51A of the UAPA shall be issued by the Central [designated] Nodal Officer for the UAPA without delay and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA Nodal Officer of the State/UT.

The order shall be issued without prior notice to the designated individual/entity.

Further, the UAPA Nodal Officer of the State/UT shall cause to monitor the transactions/ accounts of the designated individual/entity so as to 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. The UAPA Nodal Officer of the State/UT shall, upon becoming aware of any transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State/UT for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967.

F. Regarding the real-estate agents, dealers of precious metals/stones (DPMS) and other Designated Non-Financial Businesses and Professions (DNFBPs):

(i) The Designated Non-Financial Businesses and Professions (DNFBPs), inter alia, include casinos, real estate agents, dealers in precious metals/stones (DPMS), lawyers/notaries, accountants, company service providers and societies/ firms and non-profit organizations. The list of designated entities/individuals should be circulated to all DNFBPs by the concerned Regulators without delay.

(ii) The CBIC shall advise the dealers of precious metals/stones (DPMS) that if any designated individual/entity approaches them for sale/purchase of precious metals/stones or attempts to undertake such transactions the dealer should not carry out such transaction and without delay inform the CBIC, who in turn follow the similar procedure as laid down in the paragraphs above.

(iii) The UAPA Nodal Officer of the State/UT shall advise the Registrar of Societies/ Firms/ non-profit organizations that if any designated individual/ entity is a shareholder/ member/ partner/ director/ settler/ trustee/ beneficiary/ beneficial owner of any society/ partnership firm/ trust/ non-profit organization, then the Registrar should inform the UAPA Nodal Officer of the State/UT without delay, who will, in turn, follow the procedure as laid down in the paragraphs above. The Registrar should also be advised that no societies/ firms/ non-profit organizations should be allowed to be registered, if any of the designated individual/ entity is a director/ partner/ office bearer/ trustee/ settler/ beneficiary or beneficial owner of such juridical person and in case such request is received, then the Registrar shall inform the UAPA Nodal Officer of the concerned State/UT without delay, who will, in turn, follow the procedure laid down in the paragraphs above.

(iv) The UAPA Nodal Officer of the State/UT shall also advise appropriate department of the State/UT, administering the operations relating to Casinos, to ensure that the designated individuals/ entities should not be allowed to own or have beneficial ownership in any Casino operation. Further, if any designated individual/ entity visits or participates in any game in the Casino and/ or if any assets of such designated individual/ entity is with the Casino operator, and of the particulars of any client matches with the particulars of designated individuals/ entities, the Casino owner shall inform the UAPA Nodal Officer of the State/UT without delay, who shall in turn follow the procedure laid down in paragraphs above.

(v) The Ministry of Corporate Affairs shall issue an appropriate order to the Institute of Chartered Accountants of India, Institute of Cost and Works Accountants of India and Institute of Company Secretaries of India (ICSI) requesting them to sensitize their respective members to the provisions of Section 51A of UAPA, so that if any designated individual/entity approaches them, for entering/ investing in the financial sector and/or immovable property, or they are holding or managing any assets/ resources of Designated individual/ entities, then the member shall convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in paragraphs above.

(vi) The members of these institutes should also be sensitized that if they have arranged for or have been approached for incorporation/ formation/ registration of any company, limited

liability firm, partnership firm, society, trust, association where any of designated individual/ entity is a director/ shareholder/ member of a company/ society/ association or partner in a firm or settler/ trustee or beneficiary of a trust or a beneficial owner of a juridical person, then the member of the institute should not incorporate/ form/ register such juridical person and should convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in paragraphs above.

(vii) In addition, the member of the ICSI be sensitized that if he/she is Company Secretary or is holding any managerial position where any of designated individual/ entity is a Director and/or Shareholder or having beneficial ownership of any such juridical person then the member should convey the complete details of such designated individual/ entity to UAPA Nodal Officer in the Ministry of Corporate Affairs who shall in turn follow the similar procedure as laid down in paragraphs above.

(viii) The Registrar of Companies (ROC) may be advised that in case any designated individual/ entity is a shareholder/ director/ whole time director in any company registered with ROC or beneficial owner of such company, then the ROC should convey the complete details of such designated individual/ entity, as per the procedure mentioned in paragraphs above. This procedure shall also be followed in case of any designated individual/ entity being a partner of Limited Liabilities Partnership Firms registered with ROC or beneficial owner of such firms. Further the ROC may be advised that no company or limited liability Partnership firm shall be allowed to be registered if any of the designated individual/ entity is the Director/ Promoter/ Partner or beneficial owner of such company or firm and in case such a request received the ROC should inform the UAPA Nodal Officer in the Ministry of Corporate Affairs who in turn shall follow the similar procedure as laid down in paragraphs above.

G. Regarding implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001:

The U.N. Security Council Resolution No.1373 of 2001 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

To give effect to the requests of foreign countries under the U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the Central [designated] Nodal Officer for the UAPA for freezing of funds or other assets.

The UAPA nodal officer of CTCR Division of MHA, shall cause the request to be examined, within five working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances

terrorism or a terrorist organization, and upon his satisfaction, request shall be electronically forwarded to the nodal officer in RBI. The proposed designee, as mentioned above shall be treated as designated individuals / entities

The Central [designated] Nodal Officer for the UAPA shall cause the request to be examined without delay, so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the Nodal Officers in Regulators, FIU-IND and to the Nodal Officers of the States/UTs. The proposed designee, as mentioned above would be treated as designated individuals/entities.

Upon receipt of the requests by these Nodal Officers from the Central [designated] Nodal Officer for the UAPA, the similar procedure as enumerated at paragraphs above shall be followed.

The freezing orders shall be issued without prior notice to the designated persons involved.

H. Regarding exemption, to be granted to the above orders in accordance with UNSCR 1452.

The above provisions shall not apply to funds and other financial assets or economic resources that have been determined by the Central [designated] nodal officer of the UAPA to be:-

(i) necessary for basic expenses, including payments for foodstuff, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges, or exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services or fees or service charges for routine holding or maintenance of frozen funds or other financial assets or economic resources, after notification by the MEA of the intention to authorize, where appropriate, access to such funds, assets or resources and in the absence of a negative decision within 48 hours of such notification;

(ii) Necessary for extraordinary expenses, provided that such determination has been notified by the MEA;

The addition may be allowed to accounts of the designated individuals/ entities subject to the provisions of paragraph 10 of:

(a) Interest or other earnings due on those accounts, or

(b) Payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of resolutions 1267 (1999), 1333 (2000), or 1390 (2002),

Provided that any such interest, other earnings and payments continue to be subject to those provisions;

I. Regarding 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 concerned bank, stock exchanges/ depositories, intermediaries regulated by SEBI,

insurance companies, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the UAPA Nodal Officers of State/UT.

The banks, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the State/ UT Nodal Officers 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 Central [designated] Nodal Officer for the UAPA as per the contact details given in Paragraph 3.1 above, within two working days.

The Central [designated] Nodal Officer for the UAPA shall cause such verification, as may be required on the basis of the evidence furnished by the individual/entity, and, if satisfied, he/she shall pass an order, without delay, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant, under intimation to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance company, Registrar of Immovable Properties, ROC, Regulators of DNFBPs and the UAPA Nodal Officer of State/UT. However, if it is not possible for any reason to pass an Order unfreezing the assets within 5 working days, the Central [designated] Nodal Officer for the UAPA shall inform the applicant expeditiously.

J. Regarding prevention of entry into or transit through India:

As regards prevention of entry into or transit through India of the designated individuals, the UAPA Nodal Officer in the Foreigners Division of MHA, shall forward the designated lists to the immigration authorities and security agencies with a request to prevent the entry into or the transit through India. The order shall take place without prior notice to the designated individuals/entities.

The immigration authorities shall ensure strict compliance of the order and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the UAPA Nodal Officer in Foreigners Division of MHA.

K. Procedure for communication of compliance of action taken under Section 51A: The Central [designated] Nodal Officer for the UAPA and the Nodal Officer in the Foreigners Division, MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities frozen by an order, and details of the individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs for onward communication to the United Nations.

L. Communication of the Order issued under Section 51A of Unlawful Activities (Prevention) Act, 1967: The order issued under Section 51A of the Unlawful Activities (Prevention) Act, 1967 by the Central [designated] Nodal Officer for the UAPA relating to funds, financial assets or economic resources or related services, shall be communicated to all the UAPA nodal officers in the country, the Regulators of Financial Services, FIU-IND and DNFBPs, banks, depositories/stock exchanges, intermediaries regulated by SEBI, Registrars performing the work of registering immovable properties through the UAPA Nodal Officer of the State/UT.

M. Period for presenting payment instruments

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

N. Operation of Bank Accounts & Money Mules

"Money Mules" can be used to launder the proceeds of fraud schemes (e.g. phishing and identity theft) by criminal who gain illegal access to deposit accounts by recruiting third parties to act as "money mules". In some cases third parties may be innocent while in others they may be having complicity with the criminals. The instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimise the operations of "Money Mules" which are used to launder the proceeds of fraud schemes (*e.g.,* phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties which act as "money mules." If it is established that an account opened and operated is that of a Money Mule, it shall be deemed that the bank has not complied with these directions.

O. Collection of Account Payee Cheques

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

(i) A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing customers by banks.

(ii) The banks shall, at its option, not issue UCIC to all walk-in/occasional customers such as buyers of pre-paid instruments/purchasers of third party products provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

P. Issue and Payment of Demand Drafts, etc.,

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

Further, the name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheque, etc., by the issuing bank. These instructions shall take effect for such instruments issued on or after September 15, 2018.

Q. At-par cheque facility availed by co-operative banks

(i) The 'at par' cheque facility offered by commercial banks to co-operative banks shall be monitored and such arrangements be reviewed to assess the risks including credit risk and reputational risk arising therefrom.

(ii) The right to verify the records maintained by the customer cooperative banks/ societies for compliance with the extant instructions on KYC and AML under such arrangements shall be retained by banks.

(iii) Cooperative Banks shall:

a. ensure that the 'at par' cheque facility is utilised only:

- for their own use,
- for their account-holders who are KYC complaint, provided that all transactions of rupees fifty thousand or more are strictly by debit to the customers' accounts,
- For walk-in customers against cash for less than rupees fifty thousand per individual.

b. maintain the following:

- records pertaining to issuance of 'at par' cheques covering, inter alia, applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheque,
- Sufficient balances/drawing arrangements with the commercial bank extending such facility for purpose of honouring such instruments.

c. ensure that 'At par' cheques issued are crossed 'account payee' irrespective of the amount involved.

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

Adequate attention shall be paid by REs to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it shall be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing new products/services/technologies. Agents used for marketing of credit cards shall also be subjected to due diligence and KYC measures.

S. Issuance of Prepaid Payment Instruments (PPIs):

PPI issuers shall ensure that the instructions issued by Department of Payment and Settlement System of Reserve Bank of India through their Master Direction are strictly adhered to.

T. Correspondent Banks

Banks shall have a policy approved by their Boards, or by a committee headed by the Chairman/CEO/MD to lay down parameters for approving correspondent banking relationships subject to the following conditions:

(i) Sufficient information in relation to the nature of business of the bank including information on management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the bank's home country shall be gathered.

(ii) Post facto approval of the Board at its next meeting shall be obtained for the proposals approved by the Committee.

(iii) The responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented.

(iv) In the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking on-going 'due diligence' on them.

(v) The correspondent bank shall ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

(vi) Correspondent relationship shall not be entered into with a shell bank.

(vii) It shall be ensured that the correspondent banks do not permit their accounts to be used by shell banks.

(vii) Banks shall be cautious with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.

(viii) Banks shall ensure that respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

Correspondent Banking - Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services may include cash / funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable through accounts; a cheque clearing etc. It is, therefore, advised to Forex Treasury Department and Foreign Exchange Department that they shall gather sufficient information to understand fully the nature of the business of the correspondent / respondent bank. Information on the other bank's management, major business activities, level of AML / CFT compliance, purpose of opening the account, identity of any third party entities that shall use the correspondent banking services, and regulatory / supervisory framework in the correspondent's / respondent's country may be of social relevance. Similarly, they shall try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. You are aware that such relationships are established only with the approval of the Board. Whenever such relationship is established, the responsibilities of each bank in correspondent banking relationship shall be clearly documented and the same be kept on record. In the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them. The correspondent bank shall also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

Bank shall gather sufficient information to understand fully the nature of the business of the correspondent / respondent bank. Information on the other bank's management, major business activities, level of AML / CFT compliance, purpose of opening the account, identity of any third party entities that shall use the services, and regulatory / supervisory framework in the respondent's country may be obtained. Similarly, Bank shall ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. Such relationships shall be established with the approval of ALCO and put up to the Board at its next meeting for post facto approval. The closing of such accounts shall be authorised by CGM-TBG and the same shall be reported to ALCO for information. The responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented. In the case of payable-through-accounts, the Bank shall be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them. The Bank shall also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

A standard questionnaire, given in ANNEXURE 4, has been prepared by the Bank based on recommendations of Wolfsburg Group, which needs to be obtained before initiating the

correspondent relationship. The following shall be ascertained while giving approval for opening of such accounts:
Sufficient information to understand fully the nature of the business of the correspondent / respondent bank Information on the other bank's management Major business activities Level of AML / CFT compliance Purpose of opening the account Identity of any third party entities that shall use the correspondent banking services Regulatory / supervisory framework in the correspondent's / respondent's country Information from publicly available source whether that bank has been subject to any money laundering or terrorist financing investigation or regulatory action.
Correspondent relationship with a "Shell Bank"
The Forex Treasury Department and Foreign Exchange Department shall refuse to enter into a correspondent relationship with a 'Shell Bank" (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group). Shell Banks are not permitted to operate in India. The Forex Treasury Department and Foreign Exchange Department shall also guard against establishing relationships with respondent foreign financial institutions that permit their accounts to be used by shell banks. Before establishing correspondent relationship with any foreign institution, bank shall take appropriate measures to satisfy ourselves that the foreign respondent institution does not permit its accounts to be used by shell banks. The bank shall be extremely cautious while continuing relationships with respondent banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing. They shall ensure that their respondent banks have anti money laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through correspondent accounts.
8.14 NGO / NPOs- NGOs are recipient of funds from foreign sources hence the bank shall apply higher level of due diligence to the accounts of Trusts, Charities, NGOs and organizations receiving donations. NGOs / NPOs promoted by United Nations shall be kept out of the purview of higher level of due diligence.
While accepting foreign contribution to the credit of accounts of an association / organization, it shall be ensured that the concerned association / organization is registered with MHA or has permission to receive such foreign contribution and that no branch other than the designated accepts the foreign contribution.
Transactions in accounts receiving large or frequent inward remittances shall be reviewed. High risk accounts are required to be reviewed subject to enhanced KYC. Authorized dealers shall not be allowed remittances to operators of money circulation schemes.
The Trusts, charities, NGOs and organizations receiving donations other that NGOs / NPOs promoted by United Nations require higher level of due diligence, as some of NGOs are recipient of funds from foreign sources, RBI has advised Banks that while accepting foreign contribution to the credit of accounts of an association / organization, it shall be ensured that the concerned association / organization is registered with MHA or has permission to receive such foreign contribution and that no branch other than the designated accepts the foreign contribution.
Transactions in accounts receiving large or frequent inward remittances are required to be reviewed. High risk accounts are required to be reviewed subject to enhanced KYC. RBI has highlighted that remittances by authorized dealers to operators of money circulation schemes shall not be allowed.

U. Wire transfer

REs shall ensure the following while effecting wire transfer:

(i) All cross-border wire transfers including transactions using credit or debit card shall be accompanied by accurate and meaningful originator information such as name, address and account number or a unique reference number, as prevalent in the country concerned in the absence of account.

Exception: Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions shall be exempt from the above requirements.

(ii) Domestic wire transfers of rupees fifty thousand and above shall be accompanied by originator information such as name, address and account number.

(iii) Customer Identification shall be made if a customer is intentionally structuring wire transfer below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish his identity and STR shall be made to FIU-IND.

(iv) Complete originator information relating to qualifying wire transfers shall be preserved at least for a period of five years by the ordering bank.

(v) A bank processing as an intermediary element of a chain of wire transfers shall ensure that all originator information accompanying a wire transfer is retained with the transfer.

(vi) The receiving intermediary bank shall transfer full originator information accompanying a cross-border wire transfer and preserve the same for at least five years if the same cannot be sent with a related domestic wire transfer, due to technical limitations.

(vii) All the information on the originator of wire transfers shall be immediately made available to appropriate law enforcement and/or prosecutorial authorities on receiving such requests.

(viii) Effective risk-based procedures to identify wire transfers lacking complete originator information shall be in place at a beneficiary bank.

(ix) Beneficiary bank shall report transaction lacking complete originator information to FIU-IND as a suspicious transaction.

(x) The beneficiary bank shall seek detailed information of the fund remitter with the ordering bank and if the ordering bank fails to furnish information on the remitter, the beneficiary shall consider restricting or terminating its business relationship with the ordering bank.

In accordance with the RBI letter no. RBI/ 2023-24/25 dated 04/05/2023- Amendment to the Master Direction (MD) on KYC – Instructions on Wire Transfer: -

Wire Transfer:

A. Information requirements for wire transfers for the purpose of this Master Direction:

i. All cross-border wire transfers shall be accompanied by accurate, complete, and meaningful originator and beneficiary information as mentioned below:

a] name of the originator.

b] the originator account number where such an account is used to process the transaction.

c] the originator's address, or national identity number, or customer identification number, or date and place of birth.

d] name of the beneficiary; and the beneficiary account number where such an account is used to process the transaction.

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

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

iii. Domestic wire transfer, where the originator is an account holder of the ordering RE, shall be accompanied by originator and beneficiary information, as indicated for cross-border wire transfers in (i) and (ii) above.

iv. Domestic wire transfers of rupees fifty thousand and above, where the originator is not an account holder of the ordering RE, shall also be accompanied by originator and beneficiary information as indicated for cross-border wire transfers.

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

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

Any transfer that flows from a transaction carried out using a credit card / debit card / Prepaid Payment Instrument (PPI), including through a token or any other similar reference string associated with the card / PPI, for the purchase of goods or services, so long as the credit or debit card number or PPI id or reference number accompanies all transfers flowing from the transaction. However, when a credit or debit card or PPI is used as a payment system to effect a person-to-person wire transfer, the wire transfer instructions shall apply to such transactions and the necessary information should be included in the message.

Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are regulated financial institutions acting on their own behalf.

It is, however, clarified that nothing within these instructions will impact the obligation of an RE to comply with applicable reporting requirements under PML Act, 2002, and the Rules made thereunder, or any other statutory requirement in force.

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

i. Ordering RE:

The ordering RE shall ensure that all cross-border and qualifying domestic wire transfers {viz., transactions as per clauses (iii) and (iv) of paragraph 'A' above}, contain required and accurate originator information and required beneficiary information, as indicated above.

Customer Identification shall be made if a customer, who is not an account holder of the ordering RE, is intentionally structuring domestic wire transfers below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish identity and if the same transaction is found to be suspicious, STR may be filed with FIU--IND in accordance with the PML Rules.

Ordering RE shall not execute the wire transfer if it is not able to comply with the requirements stipulated in this section.

ii. Intermediary RE:

RE processing an intermediary element of a chain of wire transfers shall ensure that all originator and beneficiary information accompanying a wire transfer is retained with the transfer.

Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary RE shall keep a record, for at least five years, of all the information received from the ordering financial institution or another intermediary RE.

Intermediary RE shall take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing.

Intermediary RE shall have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

iii. Beneficiary RE:

Beneficiary RE shall take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers and qualifying domestic wire transfers {viz., transactions as per clauses (iii) and (iv) of paragraph 'A' above}, that lack required originator information or required beneficiary information.

Beneficiary RE shall have effective risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action follow-up action including seeking further information and if the transaction is found to be suspicious, reporting to FIU-IND in accordance with the PML Rules.

iv. Money Transfer Service Scheme (MTSS) providers are required to comply with all of the relevant requirements of this Section, whether they are providing services directly or through their agents. In the case of a MTSS provider that controls both the ordering and the beneficiary side of a wire transfer, the MTSS provider: shall take into account all the

information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and shall file an STR with FIU, in accordance with the PML Rules, if a transaction is found to be suspicious.

C. Other Obligations:

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

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

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

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

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

ii. REs' responsibility while undertaking cross-border wire transfer with respect to name screening (such that they do not process cross-border transactions of designated persons and entities)

REs are prohibited from conducting transactions with designated persons and entities and accordingly, in addition to compliance with Chapter IX of the Master Direction, REs shall ensure that they do not process cross-border transactions of designated persons and entities.

iii. Bank's responsibility to fulfil record management requirements.

Complete originator and beneficiary information relating to wire transfers shall be preserved by the REs involved in the wire transfer, in accordance with Section 46 of the Master Direction.

(Section 46) For the purpose of this Section, the expressions "records pertaining to the identification", "identification records", etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

V. CFT PROCEDURAL GUIDELINES

Procedural Guidelines are given for Category B Branches dealing in Foreign Exchange and Foreign Exchange Department.

i. Before undertaking any Forex transaction, they shall match the name of foreign entity with the UN sanction list, OFAC list and internal list available in AML application software. If the name matches with the above list, they shall follow the procedure given in the para (2) of the policy.
ii. The threshold limits given below are as per present RBI guidelines which are subject to change from time to time. If there is any change, the same shall be applicable for the purpose of these Policy Guidelines.

i) Imports:
a. Cash shall not be accepted for payment of import bill or advance remittance for import.
b. Collection of import bills as well as advance remittance for imports shall be done after obtaining a certificate from the Branch stating the following:

- Importer is a customer of the branch having KYC compliant account.
- The goods being imported are commensurate with the type and scale of the activity of the importer.

c. Customer's request approved by the Branch Head.
ii) Exports:
It shall be that export related receipts through Online Payment Gateway Service Providers (OPGSPs) shall not be processed for more than USD.3000.00, the ceiling prescribed by RBI.
iii) Remittances:
Inward Remittance- It shall be ensured that-
a. The remittance received shall be credited only to KYC compliant account of the beneficiary maintained with our Bank.
b. The remittance received is not originated from the non-cooperative country as per FATF Statement.
c. All wire transfer messages must be accompanied by accurate and meaningful information or as pre prescribed format of the remittance.
Remittance received under Money Transfer Scheme – X-press Money / Money Gram / Western Union:
a. A single transaction shall not be more than USD 2500 or its equivalent.
b. Frequency of remittance shall not be more than 30 times in a calendar year.
c. Remittance for more than Rs.50000.00 shall not be paid in cash. It may, however, be paid by issue of Pay Order / Demand Draft or by credit to account of beneficiary.
d. KYC / AML norms shall be followed before making a payment to the beneficiary.
All records / documents pertaining to remittance shall be maintained by the Branches and Foreign Exchange Department for ten years from the transaction date.

Outward Remittance:
All remittances shall be made as per Current Account Rule of GOI and after obtaining Application Form prescribed by the Bank. Wherever possible the documentary evidence shall be obtained from the customer, who is having a KYC compliant account, giving the details of remittance to be made.
No cash shall be accepted for issue of exchange for more than Rs.50, 000.00.

Liberalized Remittance Scheme (LRS):
It shall be ensured that:

i. The requisite application form as prescribed by the RBI shall be obtained from the applicant.
ii. The facility under LRS shall be extended to the Resident customers only.
iii. The remitter shall mandatorily have PAN number.
iv. The remittance shall not be made to countries identified by Financial Action Task Force (FATF) as non-co-operative countries and terrorists. The information available of FATF website www.fatf-gafi.org or being notified by the Reserve Bank from time to time.
v. The amount remitted during the financial year shall not be more than USD. 2,00,000.

NRI Accounts:

It shall be ensured that:
i. The account shall be opened only for the NRI or PIO. An NRO account can, however be opened for foreign national other than Pakistan and Bangladesh Nationals.
ii. No account in the name of NRI of Pakistani and Bangladeshi origin shall be opened without RBI permission.
iii. The accounts shall be opened only after obtaining requisite documents, passport copies, visa copy, latest photographs and address proof for local as well as foreign address.
iv. Before allowing Power of Attorney holder or Mandate holder to operate the S/B or C/C account, his identification and address proof shall be obtained as per KYC norms.

Remittance on behalf of NRI:

It shall be ensured that:

- A remittance shall be allowed to NRI from his NRO account after ensuring that the necessary documentary evidence in support of inheritance / legacy, proceeds of sale of house property etc. are obtained along with declaration from remitter and a certificate from Chartered Accountant under section 195 of Income Tax Act, 1961.
- That the remittance facility in respect of sale of proceeds of immovable property shall not be given to citizens of Pakistan, Bangladesh, Sri Lanka, China, Afghanistan, Iran, Nepal and Bhutan without RBI permission.
- That the facility of remittance of sale proceeds of other financial assets is not given to citizens of Pakistan, Bangladesh, Nepal and Bhutan without RBI permission.

W. 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.

X. Selling Third party products

REs acting as agents while selling third party products as per regulations in force from time to time shall comply with the following aspects for the purpose of these directions:
i. the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under Section 13(e) of this Directions.

ii. transaction details of sale of third party products and related records shall be maintained as prescribed in Chapter VII Section 46.

iii. AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.

iv. transactions involving rupees fifty thousand and above shall be undertaken only by:

a. debit to customers' account or against cheques; and

b. obtaining and verifying the PAN given by the account-based as well as walk-in customers.

v. Instruction at 'd' above shall also apply to sale of REs' own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.

Y. Freezing and closure of accounts

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

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

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

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

(v) If the accounts are still KYC non-compliant after six months of imposing initial 'partial freezing' banks/FIs should disallow all debits and credits from/to the accounts thereby, rendering them inoperative.

(vi) Further, it would always be open to the bank/FI to close the account of such customers after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions, however, need to be taken at a reasonably senior level.

In the circumstances when a bank believes that it would no longer be satisfied about the true identity of the account holder, the bank should file a Suspicious Transaction Report (STR) with Financial Intelligence Unit – India (FIU-IND) under Department of Revenue, Ministry of Finance, Government of India.

In accordance with the addition in the Master Directions KYC-2016 dated 25/02/2016, last updated on 04/05/2023, the changed address for communication is given below.

Annex II: File No. 14014/01/2019/CFT, Government of India Ministry of Home Affairs CTCR Division North Block, New Delhi. Dated: the 2nd February, 2021

(Amended vide corrigendum dated March 15, 2023),

ORDER, - Procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967.

Have amendments in sec. 10.3(a) (b) and sec. 11.A.

5.3.13- Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

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

(a) Bank shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India (Annex III of this Master Direction).

(b) In accordance with paragraph 3 of the aforementioned Order, bank shall not carry out transactions if the particulars of the individual / entity match with the particulars in the d esignated list.

Herein after we should total freeze the accounts in case the particulars of the individual / entity match with the particulars in the designated list.

(c) Further, bank should run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc. i.e., On every occasion of updating the sanctioned lists in software, the system should mandatorily verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc. with us.

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

In exercise of the powers conferred under Section 7(1) of the Act, the Central Government assigns Director, FIU-India, Department of Revenue, Ministry of Finance, as the authority to exercise powers under Section 12A of the Act. The Director, FIU-India shall be hereby referred to as the Central Nodal Officer (CNO) for the purpose of this order. [Telephone Number: 011-23314458, 011-23314435, 011-23314459 (FAX), email address: dir@fiuindia.gov.in].

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

Hereinafter the designated list, as amended from time to time, available on the portal of FIU-India, will be updated every time along with the UN and OFAC lists.

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

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

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

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

Hereinafter the designated list, as amended from time to time, available on https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm, will be updated every time along with the UN and OFAC lists.

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

10.3(a): The designated individual or organization may submit a request to the Central [Designated] Nodal Officer for UAPA under the provisions of Para 10.1 above. The Central [Designated] Nodal Officer for UAPA may be approached by post at "Additional Secretary (CTCR), North Block, New Delhi – 110001" or through email to jsctcr-mha@gov.in"

(b): The Central [Designated] Nodal Officer for UAPA shall examine such requests, in consultation with the Law Enforcement Agencies and other Security Agencies and Intelligence Agencies and, if accepted, communicate the same, if applicable, to the Ministry of External Affairs, Government of India for notifying the committee established pursuant to UNSC Resolution 1267 (1999) of the intention to authorize, access to such funds, assets or resources in terms of Para 10.1 above.

11A. Regarding procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/organizations in the event of delisting by the UNSCR 1267 (1999), 1988 (2011) and 1989 (2011) Committee,

Upon making an application in writing by the concerned individual/organization, to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, ROC, Regulators of DNFBPs, Department of Posts and the UAPA Nodal Officers of all States/UTs., who in turn shall forward the application along with the full details of the assets frozen to the Central [Designated] Nodal Officer for UAPA within two working days. The Central [Designated] Nodal Officer for UAPA shall examine the request in consultation with the Law Enforcement Agencies and other Security Agencies and Intelligence Agencies and cause such verification as may be required and if satisfied, shall pass an order, without delay, unfreezing the funds, financial assets or economic resources or related services owned or held by the applicant under intimation to

concerned bank, stock exchanges/ depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, ROC, Regulators of DNFBPs, Department of Posts and the UAPA Nodal Officers of all States/UTs.

In accordance with the addition in the Master Directions KYC-2016 dated 25/02/2016, last updated on 04/05/2023, the changed address for communication is given below.

Annex III: F.No. P - 12011/2022-ES Cell-DOR, Government of India Ministry of Finance Department of Revenue New Delhi, dated the 30th January, 2023.
ORDER- Procedure for implementation of Section 12A of "The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005"
(i.e. Whole sec. 12A)

5.3.14 - General Guidelines –

In accordance with the note no.179 dated 27/01/2022, note nos. 241 and 255 dated 08/09/2022 and 30/11/2022 respectively sanctioned in the capacity of HON. CEO,

1] Customer will be made In-operative status whenever the last account under the customer is closed.

2] All such customers mentioned in point no. 1 will be weed out from system on quarterly basis.

3] Process of customer making operative from in-operative status- certificate in prescribed format presented by branches to AML cell and AML Cell will change status of customer as operative.

4] Process of customer making operative from weed out status- certificate in prescribed format presented by branches to AML cell, and AML Cell will change status of customer as operative. Rights for such corrections are given to DGM KYC-AML Cell onwards.

The general guidelines are specified below: -

i. The data regarding customer profile (i.e. customer master in OMNI3.0) should be stored for 10 years from date of customer opening with its history, migration trail with reasons, etc. It should be available at any point of time from system. This is in accordance with strict instructions given by RBI, that overwriting of data is violation of the guidelines and is not acceptable.
ii. The existing accounts opened as Minor-Guardian, 'Sukumar', Chiranjeev, etc. should be converted to regular savings account product (2201) with fully complied KYC-AML norms, whenever they become major. i.e. on the date of completion of 18 years of age. For all such existing account holders, communication should be made 3 months prior to such date, for complying with KYC-AML norms. If they are not converted into 2201 within 3 months from communication date, then they should be marked as inoperative.

iii. For new accounts that will be opened henceforth, the existence of account is upto completion of 18 years of age of account holder. All such account holders should be communicated before 3 months from closing date of account for submission of KYC documents and convert into fully complied KYC-AML account. If not, the account will be marked inoperative on completion of 18 years of age of account holder, i.e. from the date of customer becoming a major.

iv. In case of customers becoming senior citizen, they shall be communicated 3 months prior of becoming a senior citizen according to date of birth and give opportunity to take benefits available for senior citizens.

v. Association of Persons / Body of Individual (whether registered or not) – This customer type is now available in the system and all new customers, henceforth should be opened under this type only. Branches are advised to identify such existing customers and change their customer type accordingly.

vi. For all 'other than individual customers', risk categorization should be automatically marked as Medium Risk customer, from which customers mandatorily defined as high risk (as per below chart) risk should be automatically marked as high. (E.g. PEP, trust accounts, real estate, jewelers, etc.)

vii. Vernacular Declaration form as attached herewith will be used for those customers who are using their local language for communication.

viii. Post death claim settlement of deceased person/s, these customers are to be marked as in-operative and will be subsequently weeded-out.

ix. Precautions during customer opening of Bachat Gat which are registered under their apex body or registered under NGO's etc.- KYC information and documents of their apex body or NGO's etc. will suffice for KYC compliance for such legal entity customers (Bachat Gat). KYC compliance of their office bearers as related persons are mandatory. All such rights as to declare the list of all members, office bearers, any change in both, along with opening and closing of the Bachat Gat and its accounts with the bank are laid with their apex body or registered under NGO's etc. That means office bearers of such Bachat Gat's have no right to change their members / authorized signatories and also no right to open and close Bachat Gat accounts with the bank.

x. Precautions of the customer opening for salary accounts especially customers from other states. KYC-AML compliance in all respect with PAN and OVD's is mandatory for all such customers. Undertaking or letter of employer for local address will be valid for the three months only from the date of opening of such accounts, i.e. within these three months local address details should be updated on their OVDs. The only reason to open these customers is his/her JOB. In view to mitigate the KYC-AML risk, when such customers will leave or get suspended from their JOB, branch should ensure to obtain fresh or latest KYC-AML details and documents if required, OR THE CLOSURE OF SUCH ACCOUNTS by applying negative CDD measures.

xi. As per RBI letter no. 2022-2023/117 dated 16/09/2022, amended provisions in the Master Direction - Reserve Bank of India (Interest Rate on Deposits) Directions, 2016,

Co-operative banks shall not: Open a 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 organizations / agencies listed in Schedule – I.

Explanation:

For the purposes of this clause, 'political party' means an association or body of individual citizens of India, which is, or is deemed to be registered with the Election Commission of India as a political party under the Election Symbols (Reservation and Allotment) Order, 1968 as in force for the time being. (Annexure-13)

xii. One officer from every Branch will be deputed as "KYC-AML Officer" and this officer will be the single touch point for head office for KYC-AML related compliance and its follow-up.

xiii. Comprehensive reporting system would be provided by Data Center / MIS as per requirements of AML Cell for KYC AML Compliance.

xiv. Shifting of bank accounts to another center - Proof of address:- KYC once done by one branch of the bank should be valid for transfer of the account within the bank as long as full KYC procedure had been done for the concerned account.

xv. The customer should be allowed to transfer his account from one branch to another branch without restrictions. However, it has been brought to our notice that a large number of customers with transferable jobs or those who migrate for jobs are unable to produce a proof of current / permanent address while opening a bank account immediately after relocating. In view of this, it is clarified that

a. Henceforth, customers may submit only one documentary proof of address (either current or permanent) while opening a bank account or while undergoing periodic updation. In case the address mentioned as per 'proof of address' undergoes a change, fresh proof of address may be submitted to the branch within a period of six months.

The Bank may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, OVD/Consent forwarded by the customer through mail/post, etc., shall be acceptable.

The Bank shall ensure to provide acknowledgment with date of having performed KYC updation.

The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

b. In case the proof of address furnished by the customer is not the local address or address where the customer is currently residing, the UCB may take a declaration of the local address on which all correspondence will be made by them with the customer.
c. No proof is required to be submitted for such address for the purpose of correspondence. This address may be verified by the bank through 'positive confirmation' such as acknowledgment of receipt of (i) letters, cheque books, ATM card, (ii) telephonic conversation, (iii) visits etc. In the event of change in this address due to relocation or any other reason/s, customers may intimate the new address for correspondence to the UCB within two weeks of such a change.
d. While opening new accounts and while periodically updating KYC data as required in terms of paragraph 2 of this Master Circular, an undertaking to this effect should be obtained. In all these cases customers will have to produce proof of address as mentioned at (a) and (b) above.

xvi. Role of Internal Audit Department

Bank's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The compliance function shall provide an independent evaluation of the Bank's policies and procedures, including legal and regulatory requirements. Concurrent / Internal Auditors shall specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard shall be put up before the Audit Committee of the Board on quarterly intervals. Bank shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

xvii. Policy updates and review –

a. Modifications to the policy – Updation or modification to the policy shall be initiated by Principal Officer as per business requirements keeping in view the RBI guidelines on KYC / AML or based on feedback / inputs received from branches / Departments of Head Office or based on the analysis of transactions monitored in customer accounts / operational risk events. The same shall be put up for concurrence to the Executive Committee on KYC and AML. The same shall be put up for approval to the Board of Directors.
b. Review of the policy - The policy shall be put up for review to the Board of Directors once a year.

xviii. Record Management

a) An explanation has been provided in the instructions on 'Record Management' such that the expressions "records pertaining to the identification", "identification records", etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

b) Instructions have been inserted advising REs to ensure that in case of customers who are non-profit organizations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If such customers are not registered, bank shall register the details on the DARPAN Portal. REs shall also maintain such registration records for a period of five years

after the business relationship between the customer and the RE has ended or the account has been closed, whichever is later.

xx. (a) 113A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing individual customers by REs.

(b) 114The REs shall, at their option, not issue UCIC to all walk-in/occasional customers provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

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

Further, REs shall ensure:

(a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and

(b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

xix. Information Regarding limited liability partnership (LLP)

LLP means a corporate business vehicles that enables professional expertise & entrepreneurial initiative to combine & operate in flexible, innovative & efficient manner, providing benefits of limited liability while allowing its members the flexibility for organizing their internal structure as a partnership.

A limited liability partnership (LLP) is a partnership in which some or all partners (depending on the jurisdiction) have limited liabilities. It therefore exhibits elements of partnerships and corporations. In an LLP, one partner is not responsible or liable for another partner's misconduct or negligence. This is an important difference from the traditional unlimited partnership under the Partnership Act 1890, in which each partner has joint and several liability. In an LLP, some partners have a form of limited liability similar to that of the shareholders of a corporation. An LLP also contains a different level of tax liability from that of a corporation.

Sr No	Documents
1	LLP Agreement
2	PAN Card
3	Certificate of Incorporation
4	Latest Annual Return with ROC acknowledgement
5	Utility bills in the name of firm (not more than 3 months old)
6	Govt. Recognised proofs such as shop act, factory registration, service Tax, VAT registration
7	List of partners along with capital profit percentage with DIN no
8	Self-declaration of list of bankers

9	Based on self-declaration, NOC from other banks
10	Resolution to open account with list of authorised persons along with specimen signatures to operate the account, duly attested by designated partners
11	Following documents to be taken of individual partners - - PAN Passport Election Card Driving License NREGA job Card Letter issued by UIDAI or Aadhaar Card Original latest photograph

xx. The information collected from the customer for the purpose of opening of account is to be treated as confidential and not to be divulged for cross selling or any other like purposes.

xxi. Further, the name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheque, etc., by the issuing bank. These instructions shall take effect for such instruments issued on or after September 15, 2018.

xxii. It is to be ensured that the provisions of Foreign Contribution (Regulation) Act, 1976 as amended from time to time, wherever applicable, are strictly adhered to.

xxiii. As per RBI's monetary policy statement 2012-13 (pt. No 86) followed by RBI guideline dated 09.10.2012, banks are advised to initiate steps to allot UCIC number to all their customers while entering into any new relationships in the case of all individual customers to begin with, Similarly, existing individual customers may also be allotted unique customer identification code. The Reserve Bank of India has been, from time to time, issuing guidelines on KYC/AML/CFT measures. 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. This can be achieved by introducing a unique identification code for each customer.
The UCIC will help to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable to have a better approach to risk profiling of customers. It would also smoothen banking operations for the customers.
According to the above guideline and in consideration to the note sanctioned by Hon. CEO dated 25.11.2021, bank has adopted the policy as below –

Unique customer identification code to be allotted for each customer before entering into any new relationships with the bank. Accordingly, one code for two or more customers and two or more codes for one customer is not acceptable in any circumstances. PAN and Aadhaar Number should be considered as a base for allotting UCIC. One PAN / Aadhaar Number for two or more customers and vice-versa is not acceptable in any circumstances. This should be certified from the Statutory Auditors of the bank during the process of statutory audit.

xxiv. Customer purged (weed out) – As per note sanctioned by Hon. CEO dated 25.11.2021, all customers who do not have any live account under them are marked as inoperative on

quarterly basis. At the same time, data of all such customers will be purged (weed out) from customer live data. All these customers once weed out from the system will also be removed from the reporting and won't be reactivated again except in certain cases with prior approval of Dy. GM.

Note – All customers who do not have any live account under them, but customers opened as guarantors for loan accounts, guardians for minor accounts, customers who are issued lockers, related persons for legal entities, etc. should be exempted from making inoperative in the above process.)

xxv. Process for making customer operative from Inoperative.

a. Branch should verify whether the latest and updated KYC documents with the branch and if not, such documents should be obtained from the customers with self-attestation and should be verified from the authorised officer.

b. Branch should verify documents of Legal Entity customers (other than individual) and should fill the new customer profile form (if not available with the branch). Also, beneficial ownership declaration should be taken as per the bank's policy for such customers.

c. Branch should verify that 'customer type' marking (Individual / Other) is done properly in the system.

d. KYC field in Omni 3.0 should be marked as 'Y'.

e. Update KYC from the 'KYC updation module' in Omni 3.0 system.

f. Verify the risk categorization of the customer is marked as per the profession of the customer.

g. Verify whether 'Next KYC Date' in the KYC module is correct as per the risk categorization marked for the customer.

h. If in case there is no change in the KYC documents, then branch should obtain the Re-KYC Declaration form from the customer and complete the above mentioned process.

i. Branch should provide the declaration that all the above process is duly completed and send it to AML Cell for making the customer Operative.

j. After getting the declaration from the branch, customer should be marked as operative.

xvii. Working and reporting of AML Cell shall be put before the ACB and the Hon. Board of Directors as below -

a. Monthly Reporting - KYC, Re-KYC, CKYC, BO of LE, Fraud reporting to RBI, Reporting of irregular activities and attempted frauds, various reporting to FIU-IND, etc.
b. Quarterly - RBA to KYC AML Supervision Data submitted to RBI, quarterly fraud cases reporting, cases of dacoity, robbery, etc. through FMR-IV return
c. Half Yearly – Risk Assessment of Bank including customer risk assessment and its migration report.

d. Yearly reporting - RBA to KYC AML Supervision Data with 17 standard documents submitted to RBI, consolidated yearly fraud cases reporting.
Any approval required from Hon. Board of Directors or ACB, should be first put before the Hon. Board of Management for approval from March 2022.

xviii. The bank shall make the data regarding KYC AML available to all the Regulatory Authorities (RBI, FIU-IND, etc.), Law Enforcement Authorities (SEBI, Income Tax, CBI, ED, etc.), and auditors as and when required by such authorities. While providing such data caution should be taken to check the communication source and data to be provided only to authorised sources. Such data to be provided only on specific requests.

E. Bank shall ensure that decision making functions of determining compliance with KYC norms are not outsourced. However, where required, experts, including former employees, could be hired on a contractual basis subject to the Audit Committee of Board/Board being assured that such expertise does not exist within the audit function of the bank.

In the event of any of our bank's account is maintained in any other bank, all the appointed authorized signatories of that particular account are to be declared as the Beneficial Owner of that particular account. Certificate for the same will be issued with joint signature by appointed authorized signatories. For all of these accounts, the Authorized Signatories will be appointed by Hon. CEO in accordance with the power vested with him as per resolution no. 153 passed in the Hon. Board of Directors Meeting dated 27/06/2014 and as per sanctioned note by Hon. CEO, dated 08/09/2022, these authorized signatories can be treated as natural persons who holds position of senior managing officials and therefore can be treated as Beneficial Owners for that account only.

- **Relaxation for Accounts of low risk customers**

'Simplified measures' may be applied in the case of 'Low risk' customers taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved.	Additional documents deemed to be OVDs for the purpose of proof of identity where simplified measures are applied: (i) identity card with applicant's Photograph issued by Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions; (ii) Letter issued by a gazette officer, with a duly attested photograph of the person.
For the limited purpose of proof of address, the following additional documents are deemed to be OVDs where simplified measures are applied:	(a) Utility bill which is not more than two months old of any service provider (electricity, telephone, postpaid mobile phone, piped gas, water bill);

	(b) Property or Municipal Tax receipt; (c) Bank account or Post Office savings bank account statement; (d) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; (e) Letter of allotment of accommodation from employer issued by State or Central Government departments, Statutory or Regulatory bodies, Public Sector Undertakings, Scheduled Commercial Banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and (f) Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India.

- **HUF (Hindu Undivided Family)**

PAN Card of HUF Identity proof of Karta as per OVD. Aadhaar is compulsory for Karta having Permanent of Current address. Authentication of Aadhaar is Compulsory as per Govt. notification	HUF declaration duly signed by Karta and coparceners Address proof of Karta as per OVD Rubber stamp of name of HUF & Karta

Customer Identification Procedure - Documents that may be obtained from Customers:

➢ **Accounts of individuals**
a) Passport b) Driving License c) PAN Card d) Voter Identity card issued by ECI. e) Job card issued by NREGA duly signed by an officer of State Government. f) Letter issued by the UIDAI containing details of name, address and Aadhaar number.
➢ **Accounts of companies**
a) Certificate of incorporation; b) Memorandum and Articles of Association; c) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and d) An officially valid KYC document in respect of managers, officers or employees holding an attorney to transact on its behalf.

e) PAN number of the Company.

- **Accounts of partnership firms**

a) Registration certificate.
b) Partnership deed; and
c) An officially valid KYC document in respect of the person holding an attorney to transact on its behalf.
d) PAN number of the Firm

- **Accounts of trusts**

a) Registration certificate.
b) Trust deed.
c) An officially valid KYC document in respect of the person holding a power of attorney to transact on its behalf.
d) PAN number of the Trust.

- **Accounts of Unincorporated Association or body of individuals**

a) Resolution of the managing body of such association or body of individuals;
b) Power of attorney granted to him to transact on its behalf;
c) An officially valid document in respect of the person holding an attorney to transact on its behalf; and
d) Such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals.
e) PAN number of the Unincorporated Association or body of individuals.

- **Accounts of Proprietorship Concerns**

Apart from customer identification procedure as applicable to the proprietor any two of the following documents in the name of the proprietary concern would suffice:
a) Registration certificate (in the case of a registered concern)
b) Certificate / licence issued by the Municipal authorities under Shop & Establishment Act,
c) Sales and income tax returns
d) CST / VAT certificate
e) Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities
f) Licence / certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
g) The complete Income Tax return (not just the acknowledgement) in the name of the sole Proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax Authorities.

Though the default rule is that any two documents mentioned above should be provided as activity proof by a Proprietary concern, in cases where the branches are satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the branches, however, would have to

undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern.

JANATA SAHAKARI BANK LTD., PUNE - RISK CATEGORIZATION

Code	Code Description	IND/ OTH	Aml Rating	Code	Code Description	IND/ OTH	Aml Rating
1	NORMAL	1	1	46	RPG	2	2
2	STAFF	1	1	47	DDS AGENTS A/C / PIGMMY	2	2
3	PENSION	1	1	48	COUNCIL	2	2
4	TRUST ACCOUNT	2	3	49	SUIT FILED	2	3
5	REG SOCIETY	2	2	50	PARTIAL RECONCILATION	2	3
6	NRE ACCOUNT	1	2	51	VIP Cust (15 to upto 50 Lac)	2	3
7	NRO ACCOUNT	1	2	52	STUDENTS	1	1
8	H.U.F. (KARTA)	2	2	53	HOUSEWIVES	1	1
9	MINOR ACCOUNT	1	1	54	EDUCATIONAL INSTITUTES	2	2
10	SENIOR CITIZEN	1	1	55	VARDHAHASTA(CC)	2	2
11	SOLE PROPRIETOR	2	2	56	HOUSE RENOVATION LOAN	2	2
12	LTD.CO	2	2	57	SAATHI LOAN	2	2
13	COMPANY	2	2	58	UDYOG VIKAS LOAN	2	2
14	MAHILA BACHAT GAT	2	2	59	GOLD LOAN	2	2
15	STUDENT	1	1	60	REGISTERED CO-OP SOCIETY	2	2
16	Self Help Bachat Gat	2	2	61	BANKERS CHEQUE ACCOUNT	2	2
17	Rotary Club	2	2	62	DIRECTOR	1	1
18	Housing Society (Proposed)	2	2	63	VIP CUST.(ABOVE 50 LACS)	2	2
19	Association	2	3	64	OTHERS	2	2
20	Labour Union	2	2	65	APARTMENT	2	2
21	Other (Not Registered, etc.)	2	2	66	WORKER UNION	2	2
22	INSTITUTE	2	2	67	DHR	2	2
23	FOUNDATION	2	2	68	EX STAFF - SENIOR CITIZEN	1	1
24	Private Ltd.CO	2	2	69	VENUTAI CHAVAN MAHILA MAHAVIDYALAY	2	2
25	CHARITIES	2	3	70	SHRI YOGESHWARI MAHAVIDYALAYA	2	2
26	ACADEMY	2	2	71	PSE BR.A/CS	2	2
27	ORGANISATION	2	2	72	INOPERATIVE ACCOUNT	2	2
28	BANK	2	2	73	HOUSING LOAN (Residential)	2	2
29	CREDIT SOCIETY / PATSANSTHA	2	2	74	COMMERCIAL PROPERTY PURCHASE(SHOP)	2	2
30	NBFC	2	3	75	MORTGAGE (COMMERCIAL)	2	2
31	DEVELOPMENT	2	2	76	HOUSING FLAT MORTGAGE	2	2
32	MANDAL	2	3	77	AUTO RICKSHAW	2	2
33	PARISHAD	2	2	78	NGO	2	2
34	PUBLIC TRUST ACCOUNT	2	3	79	PVT. TRUST ACCOUNT	2	3
35	REGD.HSG.SOCIETY	2	2	80	POLITICALLY EXPOSED PERSON	1	3
36	NPA ACCOUNTS	2	2	81	JEWELLERS	2	3
37	PARTNERSHIP	2	2	82	PRECIOUS METAL AND STONE	2	3
38	EMI ACCOUNT	2	2	83	REAL ESTATE	2	3

39	LOCAL GOVERMENT	2	2	84	ANTIQUE	2	3
40	SEMI-GOVT. BODIES	2	2	85	RERA ESCROW	2	2
Code	**Code Description**	**IND/ OTH**	**Aml Rating**	**Code**	**Code Description**	**IND/ OTH**	**Aml Rating**
41	LAND LORD	1	2	86	FCRA	2	3
42	BANK DIRECTORS	1	1	87	WOMEN ENTERPRENUER	1	1
43	UNI DERIDENY	2	2	88	CLUB	2	2
44	NRB	2	2	89	SECTION 8 COMPANIES	2	2
45	ESIS	2	2	90	CHEMBER OF COMMERCE	2	2
				91	UN REGISTERED FIRM	2	2

(Format for account closure in case of negative CDD)

Janata Sahakari Bank Ltd., Pune

(Multi-State Scheduled Bank)
Head Office – 1444, Shukrawar Peth, Thorle Bajirao Road, Pune – 411002.

Branch Name – _____ Date -_____

In accordance with the guidelines as laid down by Reserve Bank of India and various other regulatory authorities, the following customers' due diligence has been reported as negative. Hence all the accounts (as detailed below) of the customer are hereby closed within my authority. I confirm that all the regulatory guidelines have been followed during due diligence and the customer in no case was harassed for getting the account complied with the KYC AML norms.

Name of Customer	
Customer No	
Account No	
Date of performance of CDD	
Reason for negative CDD	

Sign –

Branch Manager
Name & Code

(Format for blind person / illiterate person declaration)

Janata Sahakari Bank Ltd., Pune

(Multi-State Scheduled Bank)
Head Office – 1444, Shukrawar Peth, Thorle Bajirao Road, Pune – 411002.

Declaration of an Independence Witness

Branch Name – _____ Date -_____

In accordance with the extant guidelines of the Reserve Bank of India and other regulatory authorities, the branch officials have properly explained the rules and regulations regarding operation of the account to Mr. / Ms. _____. Also the account holder have given his / her thumb impression in front of me accepting to have understood the rules and regulations.

I declare that, I am in no way related to the above account holder.
I hold a savings / current account with your branch bearing account no. _____

Signature
Mr. / Ms. _____
Account No - _____

(Format for downloading information from CKYCR)

Janata Sahakari Bank Ltd., Pune

(Multi-State Scheduled Bank)
Head Office – 1444, Shukrawar Peth, Thorle Bajirao Road, Pune – 411002.

Consent for downloading information from CKYCR

I, the undersigned, am willing to start a customer-based relationship with your bank and for that reason wish to give my consent for downloading the information / documents stored with CKYCR for the purpose of providing KYC documents.

I hereby confirm that the documents with CKYCR are latest and updated, and the same can also be used by the bank for KYC updation (Re-KYC) process.

I hereby give my consent for the same.

Name - _____

KYC Identification Number (KIN) - _____

Permanent Account Number (PAN) - _____

Signature - _____

References –

1. Master Direction on KYC issued on 25.02.2016 and updated as and when from time to time. (Last updation on 04th May 2023),

2. Prevention of Money Laundering Act, 2002,
3. Prevention of Money Laundering (Maintenance of Records) Rules, 2005
4. Master Direction on Frauds – Detection and Reporting of Frauds issued on 01.07.2015 and updated as and when from time to time.
5. Circular by Financial Intelligence Unit (FIU-IND) on Guidelines for effective detection and reporting of suspicious transactions issued on 28.09.2020,
6. Risk Based Approach (RBA) to KYC AML – Supervision Data Requirements issued on 08.04.2021.
7. Unlawful Activities (Prevention) Act, 1967 and as and when updated from time to time.
8. Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005)
9. Master Circular issued by RBI on 'Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards / Combating Financing of Terrorism (CFT) / Obligation of banks and financial institutions under PMLA, 2002; on 01.07.2015.
10. Banking Regulation Act, 1949.
11. Foreign Exchange Management Act, 1999
12. Payment and Settlement Systems Act 2007

All SOP's

SOP for Small Account

In case an individual customer who does not possess either any of the OVDs or the documents applicable in respect of simplified procedure (as detailed at Section 22above) and desires to open a bank account, banks shall open a 'Small Account', subject to the following:

(i) The bank shall obtain a self-attested photograph from the customer.

(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.

(iii) Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account.

(iv)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.

(v) 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 "officially valid documents".

(vi)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 "officially valid documents".

(vii) The account remains operational initially for a period of twelve months which can be extended for a further period of twelve months, provided the account holder applies and furnishes evidence of having applied for any of the OVDs during the first twelve months of the opening of the said account.

(viii) The entire relaxation provisions shall be reviewed after twenty four months. That means all these accounts must be closed after 12 months, and if relaxation given as per guidelines then it must be closed after 24 months automatically. No longer should any account remain live after 24 months under new product code "Small Account" in any circumstances.

All such account holders should be communicated after 9 months from account opening date about submission of KYC documents. The customer is expected to comply with all KYC AML norms and convert the small account to a regular savings account. If such process is not done, the customer will be marked as inoperative on completion of 12 month from the date of opening of account. For making the customer operative again, the entire process of marking customer Operative from Inoperative should be strictly followed by branches in all regards. Any type of loss suffered by the customer because of marking the customer as inoperative, then the customer will be solely responsible for such loss.

SOP for KYC compliance during on-boarding of new customers

A. Branches should ensure that customers are accepted according to customer acceptance policy of the bank.
B. Customer should be identified through the information submitted in the account opening form and the documents attached with it and oral discussion with the customer.
C. During this process, branches should also ensure that expected OVDs are obtained from the customer and accordingly all the documents so obtained from the customer should be mandatorily verified from the original documents by authorised officer.
D. Entire data collected from all the above is to be correctly filled in the Customer Master in Omni3.0.
E. If required, the KYC documents are to be verified from the competent authority (like PAN from NSDL website, Aadhaar number from UIDAI website, CIN from MCA website, etc.)
F. Branch should make sure that correct marking of KYC, AML Rating according to customer type is made in the system.
G. KYC date and other data in KYC module should be updated correctly and ensure that the Next KYC date is reflected correctly according to Risk Categorization or OVD expiry date.
H. From 01.04.2022, all the fields related to KYC AML will be made mandatory while opening a new customer and all these fields will be locked after authorization of customer. Any change to these fields should be mandatorily supported by documentary evidence and will be done only at Head Office level.
I. Identification and Declaration of Beneficial Owners for all Legal Entity customers should be taken on record during on-boarding of new customer. Detailed compliance must be done as per the process mentioned below.
J. After on-boarding of new customer, CKYC process as mentioned below should be done before setting-up any account based relationship with the customers. Detailed process is mentioned below in the policy.
(Note - Amendment of periodic updation of KYC restrictions on account operations for non-compliance made in Master Direction on KYC-2016 dated. 25/02/2016 Section no. 38 as per RBI notification letter no. RBI/2021-22/29 dt.05/05/2021 as under:-
Periodic Updation of KYC – Restrictions on Account Operations for Non-compliance -
Please refer to Section 38 of the Master Direction on KYC dated February 25, 2016, in terms of which Regulated Entities (REs) have to carry out periodic updation of KYC of existing customers. Keeping in view the current COVID-19 related restrictions in various parts of the country, REs are advised that in respect of the customer accounts where periodic updation of KYC is due and pending as on date, no restrictions on operations of such account shall be imposed till December 31, 2021, for this reason alone, unless warranted under instructions of any regulator/ enforcement agency/court of law, etc. Regulated entities are also advised to continue engaging with their customers for having their KYC updated in such cases. As per RBI letter dated 30.12.2021, this period is extended up to 31.03.2022.)
(Note - Verification of Documents:-
All documents obtained for customer KYC shall be verified / checked with the original documents by the Authorised Official and he / she shall give a confirmation to this effect under his signature on the copy of the documents obtained. Branch Manager/Assistant Branch Manager shall scrutinize Account Opening Form & KYC documents for compliance of extant KYC norms of the Bank and sign the checklist accordingly. After satisfying himself / herself, the KYC shall be certified by Branch Manager /Assistant Branch Manager. Accounts

shall be opened by CBOC Department after the complete account opening form is received from the branches.
KYC or other required documents which will be downloaded from government official website or official website of issuing authorities of the documents will not require the remark 'verified from original' but will require only self-attestation and remark as 'downloaded from site' which will be duly signed by authorised officer to suffice KYC compliance. But all the process of downloading the documents will be performed in the branch office and by banks authorised officer only.)

SOP for completing C-KYC

As per RBI Master Director KYC MD, 2016 dated 25.2.2016, Bank was required to start uploading the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017, with CKYCR in terms of the provisions of the Rules ibid.
(f) REs 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.

Also, as per the above amendment dated 06.01.2021 every individual customer opened before 01.04.2017 and every legal entity customer opened before 01.04.2021 must comply with CKYC process as per sec 38 at the time of Re-KYC or KYC Updation process. CKYC process is as follows -
i. Every Individual customer opened in the bank after 01/04/2017, every Legal entity customers (other than individual) opened after 01/04/2021, must be registered along with its KYC documents, with Central KYC Records Registry (CKYCR).
ii. Customer opened in case of fix deposit, minor guardian, shareholders, locker holders, guarantors for loan, all joint account holders, all legal entity customers, all related persons of legal entity customers, in short any customer opened by whatsoever reason it may be, in any branch, must complete C-KYC process with filling up of customer profile form (in prescribed format) with KYC documents till obtaining KIN (KYC Identification Number)
iii. Collection of forms from customers, send them to CBOC dept., clear rejection or deficiencies, if any, till C-KYC process is completed and C-KYC unique identity number (KIN) is received from C-KYCR, is the total process of C-KYC. In terms of provision of Rule 9(1A) of PML Rules, the REs shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.
iv. In case of any change in KYC information and documents accordingly, then fresh customer profile template form with changed/ fresh KYC documents should be obtained and uploaded to CKYCR, for record updation. (Note- It is necessary to mention KIN on new obtained template.)
v. In accordance with RBI Master Direction on KYC dated 25.02.2016 [Sec 56(g)], RBI letter dated 24/09/2021 and IBA letter dated 18/10/2021 (issued in accordance with RBI letter 24/09/2021), it is mandatory for the Bank to share KYC identifier with the customers, in prescribed format. Once KYC identifier is generated by CKYCR, bank shall ensure that the same will be communicated to the customer. KYC Identifier details need to be shared through a password protected file when sent through email in prescribed template.

As per RBI guidelines, from 01.04.2022, bank's branches shall ensure that above mentioned KYC compliance including C-KYC compliance is mandatorily completed by the branches before opening of a new customer and establishing any account based relationship with them.
Any existing customer not registered with CKYCR, must comply with the guidelines of CKYC during Re-KYC or KYC updation of such customer.

SOP for Re-KYC

SOP for Re-KYC/ KYC Updation of all customers –
According to RBI, KYC expired customers were treated as KYC non-compliant customers, hence KYC Updation or Re-KYC process of KYC expired customers within prescribed timeframe is, a mandatory compliance and may reduce interval gap as a requirements of EDD. (i.e. Enhance Due Diligence)
i. As per guidelines given by RBI, Re-KYC/ KYC Updation process must be done for high risk customers – once in every two years, for Medium risk customers – Once in every eight years, for Low risk customers – Once in every ten years, from opening of customers. In accordance with this KYC date expired customers, are treated as KYC non-compliant customers.
ii. Customers' KYC expiry date, would be identified at least three months before KYC expire date, i.e. at branch level, at the beginning of quarter, detail report should be generated, for the customers whose KYC will expire within the particular quarter, and all compliance for Re-KYC/ KYC Updation is mandatorily to be done within three months timeframe. For Re-KYC/ KYC Updation compliance, priority should be given as per risk categorization, i.e. High, Medium, Low, respectively.
All such customers, who's KYC will expire, should be conveyed to comply with Re-KYC process (submitting fresh KYC documents with customer profile form or Re-KYC declaration form). Henceforth, message of KYC expiry to the customer should be conveyed at least 90 days before the KYC expiry date.

In Re-KYC/ KYC Updation process, following points should be strictly complied with,
i. Obtain new templates of customer profile from customer, if not on records.
ii. Obtain latest KYC documents from customer, if not on record or had any change in already obtained KYC documents.
iii. Confirm correct information & marking in customer master (3.0 Omni) regarding, PAN no., Aadhaar no., address, mail id., mob.no., customer type (individual/ other), KYC marking (Y/N), Risk rating (1/ 2/ 3), Profession, Customer type (HUF, minor, trust, company, firm, AOP, BOI etc.), Income range, Transaction range, etc.
iv. Obtain beneficial owner declaration form for all Legal Entity customers, most of the cases it should be match with resolution in respect of Authorised signatories for account operations.
v. KYC information update through KYC Module updation in Omni 3.0 system.
vi. Confirm that the KYC Date and next KYC date (KYC expired date) is in accordance with the Risk categorization/ AML rating.
vii. If there is no any change in KYC documents and KYC related information as per branch record, then we should obtain Re-KYC Declaration form, from customers instead of taking fresh KYC documents. (Form is available in Omni 3.0 system)

viii. At the time of initiate activity of closing the last account under any customer, this customer should be converted from operative to in-operative on real time basis.
ix. All such inoperative customers (customers having no live account), shall be totally weed out from system, at the end of each quarter.
x. Data of all weed out customers should be preserved in perched format. Information of these customers should be available at any time at DR Site level.
xi. Re-KYC or KYC updation process should be very easy, customer friendly, i.e. customer shall have easy access to know his/her present KYC details. If any deficiency is found in the same or if any additional information is required, or if there is no change in KYC, then, Re-KYC declaration form shall be easily availability to the customer. For this and as a matter of huge quantum for compliance, we must take help of technology like, SMS, email, ATMs, online and internet banking, mobile applications, website, tab banking, etc.
Also, information should be given to customers about importance of Re-KYC along with the procedure for completing it through, Facebook, Instagram, YouTube official channel, etc.
xii. Every Individual customer opened in the bank before and after 01/01/2017, every Legal entity customers (other than individual) opened before and after 01/04/2021, must be registered along with its KYC documents, with Central KYC Records Registry (CKYCR) at the time of RE-KYC i.e. KYC Updation process, as per sec. 38 of MD KYC -2016. (While performing RE-KYC process, customer profile form with fresh KYC documents obtain from customer, at branch level, and should complete process of C-KYC.)
Re-KYC/ periodic updation process should be followed strictly as per sec. 38 of KYC MD-2016 dt. 25/02/2016 and as & when updated.
xiii. KYC or other required documents which will be downloaded from government official website or official website of issuing authorities of the documents will not require the remark 'verified from original' but will require only self-attestation and remark as 'downloaded from site' which will be duly signed by authorised officer to suffice KYC compliance. But all the process of downloading will be performed in the branch office and by banks authorized officer only.

Taking into consideration the quantum of compliance to be done in accordance with Re-KYC, compliance should be bifurcated into 2 parts as
i. Customers due for Re-KYC after 01.04.2022
ii. Customers pending for Re-KYC on 31.03.2022 (i.e. KYC expired customers)

i. <u>Customers due for Re-KYC after 01.04.2022</u>

Detail future date report is available in Omni 3.0 for customers who's KYC will expire after 01.04.2022. (i.e. customers' who's KYC will expire between 01.04.2022 to 30.06.2022, said report will be available on 01.04.2022). From 01.04.2022, branches should ensure that there will be no customer pending for Re-KYC as on any quarter end date.

ii. <u>Customers pending for Re-KYC on 31.03.2022 (i.e. KYC expired customers)</u>

For compliance of Re-KYC for customers who's KYC is already expired prior to 31.03.2022 should be complied with on priority basis. For this, first priority should be given to high risk customers, then to medium risk customers and lastly low risk customers.

The above mentioned process should be followed strictly by all the branches and should not be deviated at any cost.

Branches should be very careful while performing the process of Re-KYC / KYC updation that to comply with the whole beneficial ownership process as mentioned in this policy.

Beneficial Owner (BO) – Guideline and SOP

BO declaration form -

As per RBI guidelines, declaring beneficial ownership is mandatory for legal entity customers (other than individuals). From 01/04/2021 BO declaration form is a part of customer profile form. So all branches should mandatorily comply with the same while opening of such new customers. The field is also newly introduced in customer master in OMNI3.0 and is mandatory for opening a new customer.

Policy for Beneficial ownership of legal entity customers: Identification and compliance,

Types of Beneficial Owners (BO)

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

Explanation For the purpose of this sub clause-

a. "Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.

b. "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.

ii. Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent of capital or profits of the partnership.

iii. Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

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

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

As per Reserve Bank of India circular dated 08.09.2021 and IBA – Indian Bank Association's letter dated 16.12.2019, all customers other than individual like company account, partnership firms, trust, HUF, Body of Individuals, Association of Persons, etc. are legal entity customers and are required to declare the beneficial ownership in prescribed format. The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.

In short, all customers other than individual customers are Legal entity customers and mandatory compliance regarding beneficial ownership for these customers is to get duly filled declaration form in prescribed format and fill the information in Customer master, in beneficial owners / authorised signatories field in Omni 3.0 system. For all such customers, KYC documents are mandatorily to be taken for legal entity as well as related persons and update KYC module accordingly and confirm KYC and Next KYC date as per risk categorization. Branches should verify that there is similarity in the authorised signatories (AS) and beneficial owners of legal entity customers, however there can be certain exceptions for this.

Considering the above exception, in case of difference between BO and AS, then beneficial owners should be filled first followed by authorised signatories in BO / AS field in the system. Also each name should be clearly specified as BO or AS in the system by mentioning in brackets whether the person is BO or AS. [E.g. Mr. ABC (BO), Ms CDE (BO), Mr FGH (AS), Ms IJK (AS)]

Whenever any customer submits a change in the beneficial ownership, then the entire above process needs to be mandatorily be completed right from obtaining kyc documents with customer profile form till compliance of KYC, CKYC, AML, updation in Omni 3.0.

Branches should be very careful while performing the process of Re-KYC / KYC updation that to comply with the whole beneficial ownership process as mentioned above.

In the event of any of our bank account maintained in any other bank, all the appointed authorised signatories of that particular account are to be declared as the Beneficial Owner of that particular account. Certificate for the same will be issued with joint signature by appointed authorised signatories. For all of these accounts, the Authorised Signatories will be appointed by Hon. CEO in accordance with the power vested with him as per resolution no. 153 passed in the Hon. Board of Directors Meeting dated 27/06/2014 and as per sanctioned note by Hon. CEO, dated 08/09/2022, these authorised signatories can be treated as natural persons who holds position of senior managing officials and therefore can be treated as Beneficial Owners of that account only.

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:

(a) 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.

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

SOP for Risk Categorization of Customers and their Risk Migration:

Details of customer type and required risk category/ AML rating is mention in policy 2021-22. It is mandatory to give/ mark the risk category while open a customer in customer master, Omni 3.0 system.

Once Risk categorization done in customer master Omni 3.0 system, then Risk Migration cannot be available at branch level, it is only available at Head Office level, (AML Cell or Data Center)

Cases requiring risk migration will be put before the executive committee by AML Cell. The final decision of risk migration will lie with the KYC AML Executive committee. Following are some of the examples of risk migration-

i) Recommendations from STR Committee while filing the STR's,

ii) Account became NPA then risk category should be downgraded i.e. low or medium to high, and vise-a-versa account is regular again, then risk category should be upgraded i.e. high or medium to low,

iii) Customer status changed in due course then risk categorization also changed accordingly, i.e. if customer changed its status/ type from individual to other or student to businessman then risk categorization also changed from low to medium,

iv) If fraud reported or any type of criminal and adverse reports received via media or any other source from branches, departments etc. then with the recommendations received by, STR committee and KYC committee, then risk categorization should upgraded or downgraded, accordingly.

v) Any enquiry or attachment orders received from law enforcement agencies will attract risk categorization change.

This risk migration report should be made available with branch and HO level along with all trail and history, by data center.

SOP for VRV and SDN alerts generation and clearance: (As per FIU-INDIA guidelines Dt. 28/09/2020 - Implementation of 174 alerts.)

Implementation of newly introduced 174 Red Flag Indicators (RFIs)
Ref – FIU-IND circular dated 28/09/2020. (Guidelines for effective detection and reporting of suspicious transactions) and 11/05/2021 (Guidelines for reporting STR in which suspicious credits and debits through UPI are reported)

The above letter gives direction to implement new 174 RFIs (alerts) for generation of STRs for submission to FIU-IND. It contains
Annexure 1 – List 1 – System driven scenarios (1-94 online alerts)
Annexure 2 – List 2 – Offline scenarios (95-174 – customer touch point alerts)
Annexure 3 – Monitoring scenario, thresholds setting and tuning (guideline)
Annexure 4 – Model Template for STR and Guideline for filing STRs.
Annexure 4- Model Template for STR (GOS Part) and Guideline for filing STRs - Clarification
Offline scenarios are already implemented from 30.09.2021. Outreach meeting on this subject was jointly held by FIU-IND and RBI on 20/07/2021 and was minitize wherein the timeline for implementing all the scenarios was set as 30.09.2021.

For offline scenarios register to be newly prepared and maintained namely "Offline AML Alerts" at branch level for every reported suspicious transaction.

Entire guideline with all annexures i.e. all online & offline RFIs with their threshold limits were discussed, finalized and sanctioned in various KYC AML Committee meetings.

SOP for the above is also sanctioned by Hon. Chief Executive Officer vide note dated 14.01.2022 which is duly approved by Hon Board of Directors meeting dated 31.01.2022 and is to be considered as a part of this policy. (Annexure)

All available SDN lists (UN, OFAC) on the United Nations website, Banned organizations list from MHA website and all such other lists as guided by RBI to be downloaded and sent to data center for uploading them in our AML Software minimum twice in a month including any updation (addition / deletion) according to implementation of sec 51(A) of UAPA, 1697 is received from RBI, should be sent to data center for updation on 'as and when' received basis.

Following alerts will also be generated through AML software.
i. Small Accounts with their transactions and periodicity restrictions as per RBI guidelines.
ii. Transactions, if any, from office accounts to checking accounts.
iii. Any transaction that takes place in Sukumar, Chiranjeev, Minor-Guardian accounts after completion of 18 years of age of the account holder.

Following lists are now updated as caution list in AML software for alert generation.
i. Struck off companies.
ii. Banned NGOs. (Quarterly updated list from MHA's FCRA Portal (a- Organizations who's certificate is expired; b-Organizations who's License is cancelled) to be sent to data center for updation in AML Software)
iii. Shell Companies. (Identification of shell companies to be done at branch level at regular intervals and conveyed to HO immediately.)

iv. Attachment orders / enquires / investigation notices received from law enforcement agencies. (SEBI, CBI, ED, Income Tax, Cyber Crime Branch, Court, Police, etc.)

5.3.11 - SOP for Risk Based Approach to KYC-AML Quarterly Supervision Data & Yearly Documents -

Ref:- RBI Letter Dos.CO.KYC.AML./518/11.01.069/2021-22 dated 08/04/2021.

Mutual Evaluation of all the member countries will be done by FATF, India's mutual evaluation is due to be made in the year 2022-23. National Risk Assessment would be done from FATF and risk rating will be given to the country accordingly. Such risk rating has high importance in the international market.

For such assessment, exhaustive data templates are to be submitted to RBI on quarterly basis from which RBI will give gradation / risk rating to the respective bank. So submitting accurate and integrated data is binding on the bank. Our bank is among top 10 largest urban co-operative bank in the country. So, incorrect data submission on such a large scale will have adverse effect on the mutual evaluation of the country. RBI has specially instructed large banks to take extra precautions while submitting the data. Hence, incorrect data submission will be taken adversely by RBI.

The above letter gives direction to submit quarterly data in 38 templates (charts) after 30 days from the quarter end date along with 17 yearly documents within 2.5 months from year-end date.

Timeline for submitting data for December 2020 quarter along with 4 preceding quarters i.e. Dec 19, March 20, June 20 and Sept 20 should be submitted by 31.05.2021. Data for March 2021 quarter with yearly documents to be submitted by 15.06.2021.

From above mentioned 38 templates, 20 templates will be prepared and shared with us by Infrasoft Tech company and data for 18 templates and 17 yearly documents is to be generated in-house i.e. by the bank (data to be collected from all concerned departments of the bank on quarterly basis).

For country-wise risk classification, bank should refer the country-wise risk classification as published by FATF from time to time.

Nodal Officer of the bank for all the above process is to be appointed. Joint General Manager, Audit Inspection Department will act as the Nodal Officer for the above process and is already conveyed to RBI.

The detailed description and information of each template and yearly document which will be developed in-house, i.e. 18 templates and 17 documents is sanctioned by Hon. Chief Executive Officer vide note dated 14.01.2022 which is duly approved by Hon. Board of Directors meeting dated 31.01.2022 and is to be considered as a part of this policy. (Annexure B)

Entire guideline with all annexures i.e. 38 templates and 17 documents, with their parameters and required information were discussed, finalized and sanctioned in KYC AML Committee meetings.

Following reports / returns are to be submitted to Hon BOD/ ACB and senior management covering KYC aml areas (details regarding this is also mentioned in Annexure A)-

i. Monthly Review Report a. For KYC, AML (Information regarding Re-KYC, CKYC, CCR, CTR, STR, NTR, NCRB, Vigilance, Beneficial Owner compliance, etc.); b. Regarding Frauds cases (Information related to FMR-1, FUA and FMR-4, attempt to fraud cases, irregular activities, etc.)
ii. Detailed quarterly review report for all existing fraud cases.
iii. Half yearly Risk assessment report.
iv. Suspicious Transaction Report submitted to senior management after every Committee meeting.

Risk Based Approach Supervision Data are templates and documents with exhaustive data and is to be quarterly submitted to RBI. For this submission, customers' data should be collected correctly and completely and filled in the system accordingly for proper report generation.

Providing all the data required from various departments for submission of above templates and standard documents within prescribed timeline will be the sole responsibility of the concerned department.

All foreign transactions should be identified and reported separately, it should be divided into two parts i.e. trade based transactions and non-trade based transactions. All forex transactions related to trade or business are to be reported under trade based transactions, and all other are to be reported s non-trade based transactions. Also, passing of transaction in Omni3.0 system should be done in separate newly prepared batches i.e.
i. Inward Forex Transactions – Trade based (Fx-ITB)
ii. Inward Forex Transactions – Non-Trade based (Fx-INTB)
iii. Outward Forex Transactions – Trade based (Fx-OTB)
iv. Outward Forex Transactions – Non-Trade based (Fx-ONTB)

Issuing of Letter of Credit (LCs) and Bank Guarantees (BGs) are also to be divided as Foreign LC / BG (trade based and non-trade based) and Inland LC / BG (trade based and non-trade based). This is also to be reported as per newly introduced GL Heads as under.

i. Inland BG – Trade based	i. Inland LC – Trade based
ii. Inland BG – Non-Trade based	ii. Inland LC – Non-Trade based
iii. Foreign BG – Trade based	iii. Foreign LC – Trade based
iv. Foreign BG – Non-Trade based	iv. Foreign LC – Non-Trade based