Baroda Rajasthan KshetriyaGramin Bank

Policy On

Know Your Customer (KYC) Norms

Anti- Money Laundering (AML) Standards

Combating of Financing of Terrorism (CFT)

And

Obligation of Bank under PMLA, 2002

& the Prevention of Money Laundering

(Maintenance of Records) Rules, 2005

(2022)

Operation Department

Head Office, Ajmer

INDEX

ANNEXURE TO POLICY

Sr. No.	Details	Annexure
1	Digital KYC Process	A
2	KYC documents for eligible FPIs under PIS	B
3	Procedure for implementation of Section 51- A of the Unlawful Activities (Prevention) Act, 1967	C
4	List of valid KYC Documents to be obtained for Account Opening	D
5	List of High / Medium / Low Risk Countries.	F
6	Risk Categorization Table based on Annual income / Turnover	F - 1
7	Indicative List of High / Medium risk customers	F - 2
8	Indicative List of High / Medium risk Products & Services	F - 3
9	Indicative List of High / Medium Risk Geographies	F - 4
10	Indicative list of Behavior Based Alert Indicators for Branches/ Departments	F - 5 Part- I
11	Indicative list of Alert Indicators for Branches/ Departments	F - 5 Part- II
12	Customer Profile Information	G
13	List of Companies/ Individuals identified/ suspected of carrying out MLM activities	H
14	Red Flag Indicators for Trade Based Money Laundering recommended by FIU-IND Working Group	I

Abbreviations used in the Policy	
AMLRO	Anti Money Laundering Reporting Officer
BO	Beneficial Owner
CAP	Customer Acceptance Policy
CBWT	Cross Border Wire Transfers
CCR	Counterfeit Currency Report
CDD	Customer Due Diligence
CFT	Combating Financing of Terrorism
CIP	Customer Identification Procedures
CTR	Cash Transaction Report
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU- IND	Financial Intelligence Unit- INDIA
FPI	Foreign Portfolio Investors
MLM	Multi Level Marketing
MLRO	Money Laundering Reporting Officer
NTR	Non Profit Organisation Transaction Report
PEP	Politically Exposed Person
PMLA	Prevention of Money Laundering Act
POA	Power of Attorney
PO	Principal Officer
SHG	Self Help Group
STR	Suspicious Transaction Report
UCIC	Unique Customer Identification Code

Policy on:

- **Know Your Customer (KYC) norms**
- **Anti-Money Laundering (AML) standards**
- **Combating of Financing of Terrorism (CFT) measures AND Obligation of Bank under Prevention of Money Laundering Act, (PMLA), 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules,2005.**

1. Preamble:

Our bank's existing KYC-AML-CFT policy was approved by the Board of Directors on 22.02.2021. This policy is to be reviewed in reference of RBI guidelines.

In terms of the Guidelines issued by Reserve Bank of India on Know Your Customer (KYC) Standards, Anti Money Laundering (AML) Measures and Combating Financing of Terrorism (CFT), Banks are required to put in place a comprehensive policy frame work covering KYC norms, AML standards, CFT measures and Obligation of Bank under Prevention of Money Laundering Act, (PMLA), 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

Accordingly, Model policy on KYC norms, AML standards, CFT measures and obligation of Bank under Prevention of Money Laundering Act, (PMLA), 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 implemented.

Reserve Bank of India while issuing guidelines to banks taken into account
(i)Provisions / amendments applicable to banks in PML Act 2002,
(ii)Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) Measures and Combating Financing of Terrorism (CFT) and
(iii) Incorporate aspects covered in the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision with indicative suggestions wherever considered necessary.

Reserve Bank of India has issued **Master Direction vide Circular No.DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016 (Updated as on May 10, 2021)** on Know Your Customer (KYC) Norms / Anti Money Laundering (AML) Standards / Combating Financing of Terrorism (CFT) and obligation of Banks under PMLA 2002, consolidating therein all the instructions / guidelines issued on the subject till **31st January 2016.**

This policy document is therefore prepared keeping in view consolidated guidelines of Reserve Bank of India contained in their Master **Direction** dated **February 25, 2016** and guidelines issued thereafter up to **10th May 2021.** It also incorporates Bank's approach on various aspects of compliance framework of KYC-AML-CFT.

2. Effective Date of policy

This policy will be known as KYC-AML-CFT Policy of the Bank. It will be effective from the date it is approved by the Board and will supersede the earlier Policy Guidelines in respect of KYC norms, AML standards and CFT measures.

3. Previous instructions / circulars issued by Bank

All relevant instructions/guidelines regarding KYC-AML-CFT issued by Bank are being incorporated in this policy.

4. Scope / Application of the KYC-AML-CFT Policy

The guidelines contained in this Policy will be applicable to:

a. All branches of the bank.
b. Prospective / Existing Customer opening / maintaining any type of account.
c. Mobile based banking services/Net based Banking Service.
These guidelines are to be read in conjunction with related operational guidelines issued from time to time.

- **Applicable to existing and prospective customers of the bank**

While bank will apply KYC-AML-CFT norms, standards and procedures prescribed by bank in this policy to all prospective / new customers, the same would also be applied to all existing customers without any exception.

The bank will ensure that existing accounts of Individuals, Companies, Firms, Trusts, Charities, Religious Organizations and other institutions are also subjected to KYC-AML-CFT norms, standards and procedures which would establish the identity of the natural / legal person and those of the 'Beneficial Owners'.

Similarly, the Bank will ensure that Term / Recurring Deposit Accounts of existing customers are also subjected to KYC norms / procedures at the time of renewal of the deposits if such customers are not maintaining any Savings or Current Account with the bank. However if such customers are maintaining KYC compliant savings or current accounts and their accounts have not become due for updation of their identification data, then their Term / Recurring Deposits will be linked to their KYC Compliant Savings or Current Account by having cross references and no KYC Documents would be insisted from them at the time of renewal of their deposits with the bank.

- **Applicable to Mobile/Net Based Banking Services offered by bank**

These guidelines and amendments therein issued by bank from time to time will also be applicable to Mobile Based Banking Services offered by bank.

Reserve Bank of India has issued guidelines on KYC-AML-CFT to banks under Section 35A of the Banking Regulation Act, 1949 and Rule 7 of Prevention of Money-Laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005. Hence, any contravention thereof or non-compliance by bank shall attract penalties under Banking Regulation Act.

5. Confirmation for compliance of policy guidelines by Branches and Regional Authorities

All Branches will send their confirmation **on Monthly basis** to their Regional Authorities for having complied fully with the KYC–AML-CFT guidelines of the bank while opening new accounts as well in all existing accounts in the first week of succeeding month and will preserve record thereof for inspection purpose.

All Regional Authorities will also send their confirmation **on monthly basis** to the Chief Compliance Officer/Principal Officer of the bank at Head Office for having complied fully with KYC-AML-CFT guidelines of the bank while opening new accounts as well in all old existing accounts by all their branches in the first week of succeeding month and will preserve record

of monthly confirmations received from branches as well preserve record of monthly confirmations sent to the Principal Officer for inspection purpose.

6. Policy Objectives

a. To prevent bank from being used, intentionally or unintentionally, by criminal elements for Money Laundering or Terrorist Financing Activities.

b. To enable bank to know / understand their customers and their financial dealings better which in turn help them manage their risks prudently.

c. To comply with provisions of Applicable Laws and Regulatory Guidelines.

d. To lay down explicit criteria for acceptance of customers.

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

f. To establish process and procedures for monitoring transactions and / or transactions of suspicious nature in accounts.

g. To put in place appropriate software applications and controls for generations of Alerts and detection / reporting of suspicious activities in accordance with the Regulatory requirements and guidelines.

h. To create awareness amongst all the staff members through training and other means on KYC-AML-CFT norms, standards and procedures and to provide them clarity on various aspects for enabling them to implement the Policy in its true spirit.

7. Definitions:

7.1 Customer

For the purpose of KYC Norms, a 'Customer' is defined as a person or entity that maintain an account and/or a business relationship with the Bank. In other words, a person who is engaged in a financial transaction or activity with the Bank and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.(Beneficial owner)

7.2 Person

In terms of PML Act a 'person' includes:

i. an individual,
ii. a Hindu undivided family,
iii. a company,
iv. a firm,
v. an association of persons or a body of individuals, whether incorporated or not,
vi. every artificial juridical person, not falling within any one of the above persons (i to v), and
vii. any agency, office or branch owned or controlled by any of the above persons (i to vi).

7.3 Transaction

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

a. opening of an account;

b. deposits, 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 of any contractual or other legal obligation; or

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

7.4 Central KYC Records Registry (CKYCR)

"Central KYC Records Registry" (CKYCR) means a central agency i.e. CERSAI to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

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

7.5 KYC Templates

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

7.6 Officially valid document (OVD)

"Officially valid document" (OVD) means

- The passport,
- The driving licenses,
- Proof of Possession of Aadhar number,
- The Voter's Identity Card issued by the Election Commission of India,
- Job card issued by MGNREGA duly signed by an officer of the State Government,
- Letter issued by the National Population Register containing details of name, 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:-

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

ii. Property or Municipal tax receipt;

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

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

(c) The customer 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.

Explanation: Customers, at their option, may submit one of the six OVDs for proof of identity and proof of address. (Except PAN i.e. for proof of identity only)

7.7 Principal Officer

"Principal Officer" means a designated officer nominated by the Bank who is responsible for furnishing information as per rule 8 of the PML Rules.

(a) The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

(b) The name, designation and address of the Principal Officer shall be communicated to the FIU-IND. General Manager shall be Principal Officer in our Bank.

7.8 Designated Director

"Designated Director" means a person designated by the Bank to ensure overall compliance with the obligations imposed under the Prevention of Money Laundering Amendment Act and the Rules and shall be nominated by the Board.

(a) The name, designation and address of the 'Designated Director shall be communicated to the FIU-IND.

(b) In no case, the Principal Officer shall be nominated as the "Designated Director". Chairman will be "Designated Director" in our Bank.

7.9 Suspicious transaction

"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.

7.10 Walk-in Customer

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

142.

7.11 Customer Due Diligence (CDD)

"Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner using 'Officially Valid Documents' as a 'proof of identity' and a 'proof of address'.

7.12 On-going Due Diligence:

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

7.13 Periodic Updation:

"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 of India.

7.14 Foreign Account Tax Compliance Act (FATCA)

"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.

7.15 Common Reporting Standards (CRS)

"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.

7.16 Inter Governmental Agreement (IGA)

"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.

7.17 Non-face-to-face customers

"Non-face-to-face customers" means customers who open accounts without visiting the Bank's Branches/ Offices or meeting the officials of the Bank.

7.18 Politically Exposed Persons (PEPs)

"Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/ military officers, senior executives of state-owned corporations, important political party officials, etc.

7.19 Non Profit Organizations (NPO)

Non Profit Organizations (NPO) means any entity or organization that is registered as trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.

7.20"Equivalent e-document"

"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

143.

(Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

7.21"Certified copy"

Obtaining a certified copy by the Bank 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 Bank as per the provisions contained in the Act.

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

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

7.22 Beneficial Owner (BO)

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

Explanation- For the purpose of this sub-clause-

- "Controlling ownership interest" means ownership of/entitlement to more than 25 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 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.

7.23 Digital KYC

"Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with

the latitude and longitude of the location where such live photo is being taken by an authorised officer of the Bank as per the provisions contained in the Act.

7.24 Digital Signature

"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).

7.25 Shell bank"

"Shell bank" means a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.

7.26 "Wire Transfer"

"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.

7.27 "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.

7.28"Video based Customer Identification Process (V-CIP)":

A method of customer identification by an official of the Bank by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer. Such process shall be treated as face-to-face process for the purpose of this policy.

8. Key Elements of KYC-AML-CFT Policy

a. Customer Acceptance Policy (CAP)
b. Customer Identification Procedures (CIP)
c. Monitoring of Transactions
d. Risk Management

9. Customer Acceptance Policy (CAP)

Bank has formulated a clear Customer Acceptance Policy (CAP) by laying down explicit criteria for acceptance of customers as per RBI guidelines including description of the type of customers that are likely to pose a higher than average risk to the bank. Bank should ensure the following aspects of customer relationship:

a. Bank should not open any account in anonymous or fictitious / benami name(s). i.e. account on behalf of other persons whose identity have not been disclosed or cannot be verified.

b. Bank has clearly defined parameters of risk perception to classify all customers into various Money Laundering Risk Categories (MLRC) viz. Low, Medium or High Risk at the time of the

opening their accounts. For classifying customers into various Risk Categories, bank has considered following five parameters.

1. Country of domicile of the customer and his clients
2. Mode of payments
3. Type of the customer and nature of the business activity of the customer.
4. Annual Income / Turn Over of the customer.
5. Social and financial status

Customers requiring high level of monitoring, e.g. Politically Exposed Persons (PEPs),HNI, Jewelers, Trusts etc. are considered for higher risk classification.

Bank will accept customer after verifying their identity as laid down in its Customer Identification Procedures (CIP)

c. Branches should seek 'mandatory' information required for KYC purpose which the customer is obliged to give while opening an account or during periodic updation. Other 'optional' customer details/ additional information, if required, may be obtained separately after the account is opened only with the explicit consent of the customer.

d. No transaction or account based relationship is undertaken without following the Customer Due Diligence (CDD) procedure**.** CDD Procedure is to be followed for all the joint account holders, while opening a joint account. Further, if an existing KYC compliant customer desires to open another account with our Bank, she/he need not submit fresh proof of identity and/or address. There is no need for a fresh CDD exercise

e. Bank will not open an account, where bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and / or obtain documents required as per the risk categorization due to non-co-operation of the customer or non-reliability of the data / information furnished to the bank.

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

➢ **Freezing and closure of accounts**

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

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

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

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

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

vi. Further, bank would have discretion to close the accounts of such customers after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions, however, need to be taken at a reasonably senior level. Branches should, therefore, obtain prior approval from respective Regional Authorities in this regard.

vii. When a customer is permitted to act on behalf of another person / entity, bank will ensure to examine circumstances thereof and clearly spell out the same in conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity.

- Bank has already enabled all necessary checks in system before opening a new account in Finacle, 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. In other words, Bank will not open accounts of known criminals or Terrorist Individuals /Entities / Organizations.

- Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.(see point no.30.5 General guidelines in this policy)

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

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

➢ **Customer profile**

Bank will prepare a profile for each new as well of existing customers based on their Risk Categorization. While preparing customer profile, branches should seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein should not be divulged by bank for cross selling or any other purposes. **(Annexure - G)**

The customer profile should mainly contain following information relating to customers' Identity,

a. Nationality / Country of domicile

b. Date of birth,

c. Social / Financial status,

d. Anticipated / Actual Annual income,

e. Anticipated / Actual Annual Turnover

f. Nature of business activity,

g. Information about his / her clients' business and their location and

h. Information about his / her employer and location etc.

Branches will obtain above information from the prospective customers through Account Opening Forms / Separate Forms at the time of opening their accounts. In case of existing customers, branches should obtain above information while updating their identification data at the prescribed intervals i.e. at every two years for High Risk individuals and entities. Full KYC exercise will be required to be done at every ten years for Low Risk and at every eight years for Medium Risk individuals and entities as specified in this policy.

10. Money Laundering Risk Categorization

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

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

Keeping in view above, bank has prepared

a. List of High / Medium / Low Risk Countries **(Annexure- F),**

b. Risk categorization Table based on Annual Income / Turn over in the account of the customer **(Annexure- F -1)**and

c. List of various types of customers for Money Laundering Risk Categorization. **(Annexure- F -2).**

Bank shall categorize new as well as all the existing customers into various Money Laundering Risk Categories viz. Low, Medium or High Risk on the basis of Money Laundering Risk Perceptions / parameters as mentioned in **Annexure- F-2.**

Bank shall **put stamp/ mention at the appropriate column of Money Laundering Risk Category on Account Opening Forms / Signature cards at the time of opening accounts** and KYC Forms / Documents obtained at periodical intervals for updation of identification data of the existing customers.

Assigning Money Laundering Risk category (MLRC) to customers of branches by the system itself through menu option "**RISKU**" by taking into account three risk parameters such as
(i) Country of domicile
(ii) Annual Income / Turnover in the A/c and
(iii) Type of product / service availed by the customer with a view to avoid human intervention and to have uniformity in risk categorization.

Money Laundering Risk Category (MLRC) of customers on the basis of above parameters are derived and populated / maintained by Data Center in the CBS System at free code 2 under MIS TAB in CUMM/HCUMM option for their examination purpose.

Branches will recheck / verify Money Laundering Risk Category (MLRC) assigned by the computer system keeping in view the other parameters i.e. nature of business and activity of the customer, location of his clients, mode of payments, social status for the reason that these parameters are not recognized by the computer system, but are best known to the branches including subsequent changes if any in it at a later date.

Branches will make suitable corrections if any, in Risk Category assigned by the computer system based on these parameters or any other parameters as fixed by the bank and as deemed fit to them and or give Risk Category at the time of opening the account at Free Code 1 under MIS TAB in CUMM/HCUMM option. While downloading report, the higher of the Risk Category of customer either at Free Code 1 or Free Code 2 will be taken by the system.

10.1. Review of Money Laundering Risk Category

Bank will ensure periodical review of Risk Categorization of accounts and the need for applying enhanced due diligence measures to meet with the Regulatory requirements. Such review of Risk Categorization of Customers will be carried out at a periodicity of **not less than once in six months** as directed by Reserve Bank of India. Bank will therefore review Risk Categorization in March(for half year ending March) and September(for half year ending September) every year. Bank will generate report of Money Laundering Risk Categorization and maintain proper record thereof for the purpose of inspection.

10.2. Due Diligence in Customer Accounts

Customer Due Diligence (CDD) can be defined as any measure undertaken to collect and verify information of identity proof and address proof to positively establish the identity of a customer.

Types of CDD: There are three types of CDD that can be used by the bank in accordance with the risk category of the customer. These are listed as follows:

a. Basic Due Diligence: This implies collection and verification of identity proof address proof and photograph to establish the identity of the customer.

b. Simplified Due Diligence: Any due diligence applied to establish the identity of customer, which involves measures less stringent then basic due diligence can be termed as 'Simplified Due Diligence'. As per the RBI guidelines, simplified due diligence can be applied to accounts of people belonging to low income group, both in urban as well as rural areas, to enable 'Financial Inclusion' of this segment. It can also be applied to accounts which have a financial cap, like the "Small Accounts" where the balance in the account and total credits in the account at any point of time in a year should not exceed Rs. 50,000/-.

i.)Simplified Norms for Self Help Groups (SHGs)

- KYC/CDD of all the members of SHG shall not be required while opening the savings bank account of the SHG.
- KYC verification/CDD of all the office bearers shall suffice for this purpose.
- Customer Due Diligence (CDD) of all the members of SHG may be undertaken at the time of credit linking of SHGs

ii) Procedure to be followed in respect of foreign students:

Bank will follow the following procedure for foreign students studying in India.

A) Bank shall, at their option, open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with appropriate visa & immigration endorsement) which contains the proof of identity and address in the home country along with a photograph and a letter offering admission from the educational institution in India.

i) 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.

ii) Provided further that pending 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 monthly withdrawal to Rs. 50,000/- on aggregate in the same, during the 30 day period.

B) On receipt of the proof of current address, the account would be treated as a normal NRO account, and will be operated in terms of instructions contained in the Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of FEMA1999.

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

iii)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), should be opened by accepting KYC documents (Annexure- B), subject to Income Tax (FATCA/CRS) Rules.

Provided that Branches should obtain undertaking from FPIs or the Global Custodian acting on behalf of the FPI that as and when required, the exempted documents (Annexure-B) will be submitted.

c. Enhanced Due Diligence (EDD): Any additional due diligence measures undertaken over and above the basic due diligence can be termed as 'Enhanced Due Diligence'. As per the RBI guidelines, EDD needs to be undertaken for all the high-risk customers of a bank. Enhanced Due Diligence is also built in the account opening processes at the product level or customer type level, where the high risk customers are easily identifiable (e.g. NRIs, Trust accounts, Correspondent Banking, account opened by professional intermediaries, and accounts of politically exposed persons needs enhanced due diligence)

Enhanced Due Diligence (EDD) for higher risk customer accounts

Due Diligence will be carried out depending on the risk perceived while opening new account and / or while allowing high value transactions in the existing accounts i.e. Enhanced / intensive / higher Due Diligence measures will be carried out in case of High / Medium risk customers, including those for whom the sources of funds are not clear.

Enhanced Due Diligence (EDD) is required in case of following types of High risk customers.

a. Non-resident customers;

b. High net worth individuals (HNI)

c. Trusts, Charities, NGOs and organizations receiving donations;

d. Companies having close family shareholding or beneficial ownership;

LSD.

e. Firms with 'sleeping partners';

f. Politically exposed persons (PEPs) of foreign origin / Resident outside India, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;

g. Non-face to face customers;

h. Those with dubious reputation as per public information available etc.

i. Cash intensive businesses like Bullion dealers (including sub-dealers) & Jewelers;

j. Fiduciary Accounts and

k. Pooled Accounts

➢ In case of high risk customers, banks should obtain additional information on the customer beyond documentary evidence. An indicative list is as under:

- Information on net worth
- Intended business activity in case of NRI customers
- Report by branch manager
- Higher level of approvals
- Verification of customer information with independent data sources

➢ In addition to what has been indicated above, Bank has taken steps to identify and assess its Money Laundering (ML) / Terrorist Financing (TF) risk for customers **(Annexure-F, Annexure-F-1&Annexure-F-2)**, countries and geographical areas **(Annexure-F-4)** as also for products/ services/ transactions/ delivery channels**(Annexure- F-3)**, Bank has adopted enhanced measures as per the indicative list provided by the IBA on the customer behavior and Risk Based Transaction Monitoring, High and Medium Risk Customers, IBA alerts **(Annexure- F-5)**.

However, only NPOs/NGOs promoted by United Nations and its agencies may be classified as low risk customer.

➢ **Account Opening Process Flow at Branches**

At the time of opening of the account, the branch to ensure that all the fields of the account opening form are duly filled in and obtain -

□ **"Officially Valid Documents"** as applicable as per the category of the customer **(Annexure- D)**

□ Passport size recent photographs for affixing them on the account opening form, CKYC Registry Form and pass book.

□ Specimen signature of the customer in the presence of a verifying official.

□ Instructions of the customers regarding mode of operation in the account.

□ Nomination in case of individual accounts, if not, specifically refused the facility by the customer

□ Details of accounts of the customer with other bank/s (if any)

□ Permanent Account Number (PAN) of the customer given by Income Tax authorities or Form No.60 as applicable. Online verification of PAN number should be done.

Copies of the submitted KYC documents must be verified with the originals and officials accepting such documents should invariably put a stamp "Verified with the original(s)" under his/her signature and date.

151.

The above documents/ data would help the bank to establish the identity of the person opening the account. However, for preparing risk profile of the customer, some additional details may be required such as business / employment details, source of income, annual income, assets owned, personal details such as qualification, marital status, etc. As already mentioned above, such additional information shall however be sought which is relevant to the perceived risk, is in conformity with the guidelines issued in this regard and is not intrusive. Besides, such additional information **shall be sought separately with his / her consent and after opening the account.**

i.)Client accounts opened by professional intermediaries:

a. When the bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified.
b. Bank will hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Bank will also maintain 'pooled' accounts managed by lawyers / chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients.

c. Where funds held by the intermediaries are not co-mingled at bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at branch, branch should identify the beneficial owners.

d. Where the bank relies on the 'customer due diligence' (CDD) done by an intermediary, bank will satisfy itself that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements to the customers. However, Bank has not yet engaged any third party for relying on the 'Customer Due Diligence' (CDD).

e. 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 will 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.**

f. 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 transactions will not be allowed to open an account on behalf of a client.

g. The ultimate responsibility for knowing the customer lies with the bank.

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

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, and will include

1. Heads of States or of Governments,
2. Senior politicians,
3. senior government / judicial / military officers,
4. Senior executives of state-owned corporations,

152

5. Important political party officials, etc.

Bank will have the option of establishing a relationship with PEPs provided that;

a. sufficient information including information about the source of funds, accounts of family members and closed 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.
f. Before opening an account of PEP, branches will take / obtain authority of their Regional Heads.

Also in the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP and where PEP is the ultimate beneficial owner, bank will take/ obtain approval/authority of their Regional Heads to continue business relationship and subject account to the Customer Due Diligence (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 PEP is the ultimate beneficial owner.**

g.Further bank will also perform Enhance Due Diligence to the customers, who are close relatives of PEPs, and accounts of which PEP is the ultimate beneficial owner.

iii) Accounts of non-face-to-face customers

With the introduction of phone and electronic banking, accounts are increasingly being opened by Banks for customers without the need for the customer to visit the Branch. In case of non-Face-to-Face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Branches should follow the following procedure:

a. Certification of all the documents presented.
b. If necessary, additional documents may be called for.
c. In such cases, Branches should also require the first payment to be effected through the customer's KYC compliant account with another Bank for enhanced due diligence of non-face-to-face customer.
d. In the case of cross border customers, there is additional difficulty of matching the customer with the documentation and the Branch may have to rely on third party certification. In such cases, it must be ensured that the third party is a regulated and supervised entity and KYC system is in place.

11. Customer Identification Procedure (CIP)

(A) Customer Identification means undertaking client due diligence measures while commencing an account based relationship including identifying and verifying the customer and beneficial owner on the basis of one of the Officially Valid Documents (OVDs).The branch must be able to satisfy the competent authority that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based

153.

approach is considered necessary to avoid disproportionate cost to the Bank and burdensome regime for the customers.

(B) Branches shall carry out the Customer Identification Procedure (CIP) at following stages:

i) While commencing an Account-based relationship with the customer and updating identification data of the existing customer at prescribed intervals;

ii) Carrying out any international money transfer operations for a person who is not an account holder of the Bank;
iii) When the branch has a doubt about the authenticity or adequacy of the customer identification data it has obtained;

iv) When the Branches sell third party products as agents, selling the Bank's own products, payment of dues of credit cards/sale and re-loading of prepaid/travel cards and any other product for more than Rs. 50,000/-

v) While carrying out transactions for a Non-Account based customer i.e. a walk-in customer, where the amount involved is equal to or exceeding Rs.50,000/-, whether conducted as a single transaction or several transactions that appear to be connected;
vi) When a Branch 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 Rs. 50,000/-.
vii) Branches are, therefore, advised to obtain appropriate Identity and Address documents while carrying out Customer Identification Procedure.

(C) RBI has advised that for the purpose of verifying the identity of customers at the time of commencement of an Account-based relationship, Bank shall, at its option, rely on customer due diligence done by a third party, subject to the following conditions:

i) Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.

ii) Adequate steps are taken by the Bank to satisfy itself 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;

iii) The third party is regulated, supervised and monitored 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.

iv) The third party should not be based in a country or jurisdiction assessed as High Risk;

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

In view of the above, Branches are advised not to rely on due diligence done by a third party.

(D) While undertaking customer identification, Branches should ensure that:

i) Decision-making functions of determining compliance with KYC norms are not outsourced.

ii) Branches should not seek introduction while opening accounts

iii) The customers will be asked to furnish additional OVD, if the OVD submitted by the customer doesn't contain current address of the customer.

(E) The Bank should seek "mandatory" information required for KYC purpose (Annexure- D) which the customer is obliged to give while opening an account or during periodic updation. Other "optional" customer details/ additional information, if required, will be obtained separately after the account is opened only with the explicit consent of the customer.
The customer has a right to know what is the information required for KYC that she/he is obliged to give, and what is the additional information sought by the bank i.e. optional. Bank will ensure that the information (both mandatory-before opening the account as well as optional- after opening the account) with the explicit consent of the customer.

(F) Further, bank will collect following additional information while opening new account for the purpose of identification of the customer.

a. the purpose and reason for opening the account or establishing banking relationship

b. the anticipated level and nature of the activity that is to be undertaken

c. the expected origin of the funds to be used within the relationship

d. details of occupation / employment and sources of wealth or income required for banking relationships

(G) New accounts will be personally monitored for **at least six months** by the Branch Head / designated officer to observe that the activities in respect of the account are in conformity with KYC information given by the account holder. Such Risk based approach is considered necessary by bank to avoid disproportionate cost to the bank and a burdensome regime for the customers.

(H) Besides Money Laundering Risk Perception, the nature of information /documents required would also depend on the type of customer (individual, corporate etc.). The true identity and bonafides of the existing customers and new potential customers opening accounts with the bank and obtaining basic background information would be of paramount importance.

(I) List of "Officially Valid KYC Documents" to be obtained for Account Opening:

A list of the nature and type of documents/ information that may be relied upon for Customer Identification is given in **Annexure- D**. The KYC- documents mentioned in **Annexure- D** must be accepted as 'Officially Valid Documents' by the branches while opening any new account of the prospective customers.

Branches have no discretion to accept any other document for this purpose.

(J) In case of High or Medium Risk categorized customers, bank will ask applicant to furnish more documents in respect of their identification as a measure of higher due diligence.

(K) The Correct permanent address, as referred to in Annexure-D means the address at which a person usually resides **and bank will ensure that the address given by the customer must matches with the address on the 'Officially Valid Document'.**

(L) If address on the 'Officially Valid Document' submitted for identity proof by the prospective customer is same as that declared by him/her in the account opening form, the document will be accepted as a valid proof of both identity and address.

(M) Verification of Genuineness of Address:

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

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

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

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

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

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

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

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

(R) Customers are also required to inform / intimate bank about change in their address within two weeks of such a change, either due to change in residence / locality and or place of business as the case may be along with required documentary proofs to the satisfaction of the bank. Bank will ensure to update such changes in addresses in its records / system as and when intimated / received from the customers.

(S) Verification of documents:

The identification of documents / address proof documents obtained in course of Customer Due Diligence (CDD) measures will be verified from the originals to the satisfaction of bank, and the official verifying the documents with the originals shall authenticate the copies by affixing his signature with words "Verified with Original".

Wherever bank has any doubt about genuineness of KYC documents, Bank will exercise further due diligence by

a. Personal visit to the address mentioned in the account opening form and address proof document/s or

b. Ascertaining information of the account holder from the employer of the customer.

c. Making call to the telephone number/s mentioned in the account opening form and verifying details submitted in the application by the customer.

d. If customer has either quoted PAN or submitted the copy thereof, Bank to ensure that the same is validated online with NSDL Server while opening of the account.

11.1. Unique Customer Identification Code (UCIC): The increasing complexity and volumes 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 Unique Customer Identification Code (UCIC) will help banks to identify customers, track the facilities availed,

monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers. It is also necessary for smoothening banking operations for the customers.

RBI therefore, advised banks to initiate steps for allotting UCIC to all their customers while entering into any new relationships with the customers **as well as for the existing customers also.** It is reiterated that UCIC must be allotted to all customers while entering into new relationships.

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

Bank has developed a menu "FINDCUST" to identify existing customer ID based on PAN, Mobile Number, Passport, Aadhaar, Voter ID and Driving License before creation of new Customer IDs.

Further Bank has also developed menus "CUSTDDUP"and "MERGCUST" to identify and merge existing duplicate customer IDs in the system respectively for allotment of UCIC.

Branches should ensure that multiple customer IDs are not created further and existing multiple customer IDs are merged/ suspended as per guidelines issued from time to time.

Further, the branches to ensure that there is adequate mechanism to identify walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC i.e. they should make our customer complying with the KYC-AML policy guidelines.

11.2 Customer Due Diligence requirements (CDD) while opening of accounts

11.2.1 Accounts of Individuals (Natural Persons)

For undertaking CDD, Bank will obtain the following information from an individual while establishing an Account based relationship or while dealing with the individual who is a beneficial owner, authorized signatory or the Power of Attorney holder related to any legal entity:

A) From an individual who is eligible for enrolment of Aadhaar,

i. The Aadhaar number,

- Is **mandatory** where he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Adhaar (Targeted Delivery of Financial and Other subsidies, Benefits and services) Act,2016 (18 of 2016):

Provided that where the customer has submitted

Aadhaar number under paragraph (i) above to a bank notified under first proviso to sub-section (1) of section 11A of the PML Act, bank shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India.

(**In case e-KYC authentication cannot be performed** for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, Bank shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e-document thereof from the customer. CDD done in this manner shall invariably be carried out by an official of the Bank and such exception handling shall also be a part of the

157.

concurrent audit as mandated in Section 8. Bank shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Bank and shall be available for supervisory review.

Explanation 1: Bank shall, where its customer submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such customer redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required as per provision 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

Or

- he decides to submit his Aadhaar number **voluntarily** to a bank notified under first proviso to subsection (1) of sec.11A of the PML Act:

ii. Permanent Account Number (PAN) or Form No. 60 as defined in Income-tax Rules, 1962, as amended from time to time; and

iii. Such other documents including in respect of the nature of business and financial status of the client, or the equivalent e-documents thereof as may be required by the Bank.

If an Aadhaar number has not been assigned to an individual, proof of application of enrolment for Aadhaar shall be obtained wherein the enrolment is not older than 3 months and in case PAN is not submitted, FORM 60 is mandatory and certified copy of an OVD containing details of identity and address and recent photograph shall be obtained.

Explanation- Obtaining a certified copy means that comparing the copy of officially valid document produced by the customer with the original and recording the same on the copy invariably by putting a stamp 'Verified with the original(s)' by the authorized official of the branch under his/ her signature and date.

In case of

B) From an individual who is not eligible to be enrolled for an Aadhaar number or who is not a resident, the following shall be obtained:

i. PAN or Form No. 60 as defined in Income-tax Rules, 1962, as amended from time to time.
ii. Recent photograph and
iii. A certified copy of an OVD containing details of identity and address.

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

While opening accounts of legal entities, PAN is Mandatory.

158.

- Explanation 1: Aadhaar number shall not be sought from individuals who are not 'residents' as defined under Aadhaar Act, 2016.
- Explanation 2: Customers, at their option, shall submit one of the five OVDs. (However, in case of NRIs, a copy of valid Passport / PIO / OCI card and Visa is mandatory.)

C) In case the identity information relating to the Aadhaar number or Permanent Account Number/FORM 60 submitted by the customer does not have current address, an OVD must be obtained from the customer for this purpose.

However, If the OVD furnished by the customer does not contain updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:-

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

ii. property or Municipal tax receipt;

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

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

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

- The customer is required to submit Aadhaar or OVD updated with current address within a period of -3- months of submitting above documents/opening of an account. If the customer fails to submit the same within prescribed timeline, the branch shall cease the operation in the account by freezing it till the time updated officially valid document is submitted by the customer and updated in the CBS.

D) Bank, at the time of receipt of the Aadhaar number, will carry out e-KYC authentication (biometric or OTP based). Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the bank or Yes/No authentication with the explicit consent of the customer subject to following conditions:

i. Yes/No authentication will not be carried out while establishing an account based relationship.

ii. In case of existing accounts where Yes/No authentication is carried out, Bank will ensure to carry out biometric or OTP based e-KYC authentication within a period of six months after carrying out yes/no authentication.

iii. Yes/No authentication in respect of beneficial owners of a legal entity will suffice in respect of existing accounts or while establishing an account based relationship.

iv. Where OTP based authentication is performed in 'non-face to face' mode for opening new accounts, the limitations mentioned below.

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

Explanation: While seeking explicit consent of the customer, the consent provisions, as below, must be observed.

- At the time of authentication, Bank will inform the Aadhaar number holder of the following details:-

(a) The nature of information that will be shared by the Authority upon authentication;
(b) The uses to which the information received during authentication may be put; and
(c) Alternatives to submission of identity information

- Bank will obtain the consent in physical or preferably in electronic form and maintain logs or records of the consent obtained in the manner and form as may be specified by the Authority for this purpose.

Explanation: Bank will allow the authentication to be done at any of their authorized branches.

Accounts opened using OTP based authentication is performed in 'non-face to face' mode for opening new accounts.

Accounts opened in terms of this provision i.e.; using OTP based e-KYC, are subject to the following conditions:

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

ii) The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh.

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

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

v) Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which Customer Due Diligence (CDD) procedure is to be completed by the branches. If the CDD procedure 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.

vi) 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 either with the same bank or with any other bank. Further, while uploading KYC information to CKYC, Bank will clearly indicate that such accounts are opened with OTP based e-KYC procedure and Bank shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

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

(E)Changes due to introduction of Video based Customer Identification Process (V-CIP)
Bank may undertake live V-CIP, to be carried out by an official of the Bank, for establishment of an account based relationship with an individual customer, after obtaining his informed consent and shall adhere to the following stipulations:

i. The official of the Bank performing the V-CIP shall record video as well as capture photograph of the customer present for identification and obtain the identification information as below:

- Banks: can use either OTP based Aadhaar e-KYC authentication or Offline Verification of Aadhaar for identification. Further, services of Business Correspondents (BCs) may be used by banks for aiding the V-CIP

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

iii. Live location of the customer (Geotagging) shall be captured to ensure that customer is physically present in India

iv. The official of the Bank shall ensure that photograph of the customer in the Aadhaar/PAN details matches with the customer undertaking the V-CIP and the identification details in Aadhaar/PAN shall match with the details provided by the customer.

v. The official of the Bank shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

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

vii. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of process.

viii. Bank shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audio-visual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. Bank shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

ix. To ensure security, robustness and end to end encryption, the Bank shall carry out software and security audit and validation of the V-CIP application before rolling it out.

x. The audio-visual interaction shall be triggered from the domain of the Bank itself, and not from third party service provider, if any. The V-CIP process shall be operated by officials specifically trained for this purpose. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

xi. Bank shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.

xii. Banks are encouraged to take assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer. However, the responsibility of customer identification shall rest with the Bank.

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

xiv. BCs can facilitate the process only at the customer end and as already stated above, the official at the other end of V-CIP interaction should necessarily be a bank official. 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.

The existing customer, eligible to be enrolled for Aadhaar and obtain Permanent Account Number, **is required to submit the Aadhaar number and Permanent Account Number/ Form 60 by such date as notified by the Central Government subsequently.**

In case the customer fails to submit the Aadhaar number and Permanent Account Number/Form 60 by such date, **the account will be ceased to be operational by the Branch till the time Aadhaar Number and Permanent Account Number/Form 60 is submitted by the customer**. Before freezing, Branch should ensure that at least two notices for the compliance have been issued by the Branch before freezing the account by such date **as notified by the Central Government**.

11.2.2 Introduction:

Since introduction is **not mandatory** for opening of account, branches need not to obtain introduction from the customers for opening of bank accounts.

11.3. In case of Joint Account of individuals

Applicants who are not closely related to each other would be required to establish their identity and address independently. Bank will therefore ensure to obtain separate KYC Documents as mentioned in **Annexure- D** from each of the joint account holder for establishing their identity independently. Bank will also ensure this whenever any addition of names of such individuals are requested by existing customers in their accounts.

Branches to ensure that separate Unique Customer ID is allotted to each Joint- holder of the account at the time of opening of account if he/she does not have any existing Customer ID.

11.4. In case of Foreign Students who are finding it difficult to open account in the branches of the bank, branches should obtain

a. An Identity Card along with an admission letter for the course mentioning duration of course for which he / she had been admitted by the Institute / College.

b. Copy of Passport and copy of Visa.

c. An allotment letter on letter head of Institution / College for allotting him / her hostel accommodation duly signed by the authorized signatory, mentioning detailed address and location of hostel, room no. etc. and date of allotment of hostel accommodation etc.

11.5.In case of transfer of account from one branch to another branch: KYC once done by one branch of the Bank will be valid for transfer of the account within the Bank as long as full KYC has been done for the concerned account. The customer will be allowed to transfer his account from one branch to another branch without restrictions. In order to comply with KYC requirements of correct address of the person; declaration will be obtained from him/her upon such transfer by the transferee branch.

Branches will transfer existing accounts to the transferee branch without insisting on fresh proof of address and on the basis of a self-declaration from the account holder about his/ her current address.

Bank will intimate to their customers that in the event of change in address due to relocation or any other reason; the customer should intimate the new address to the bank within two weeks of such a change.

11.6. Accounts of Non- Individuals (Legal Persons / Entities)

For customers that are Legal Persons or Entities (i.e. Firm, Company, Trust, etc.), bank will

a. Verify the legal status / existence of the legal person / entity through proper and relevant documents i.e. Obtain sufficient identification document to verify the identity of the legal entity as also of all Partners/ Directors/ Trustees/ Office Bearers who are signatory to the account opening form as mentioned in **Annexure- D.**

b. Obtain documents for correct permanent address / location of legal entity as also of all Partners/Directors/Trustees/ Office Bearers who are signatory to account opening form as mentioned in **Annexure- D.**

c. Obtain recent photographs of all Partners/Directors/Trustees/ Office Bearers who are signatory to the account opening form.

d. Also Verify that any person purporting to act on behalf of the legal person / entity so authorized and identify & verify the identity of that person as mentioned in **Annexure- D**

e. Understand the ownership and control structure of the customer and determine who are the natural persons, who ultimately control the legal person and also obtain KYC documents of the 'Beneficial Owner'.

11.6.1. Customer Identification Requirements in case of Legal Persons

Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in the following paragraph for guidance of branches. In case it is decided to accept such accounts, in terms of bank's Customer Acceptance Policy (CAP), reasonable measures will be taken by branches to identify the beneficial owner(s) and verify his/her/their identity in a manner so that branch is satisfied that it knows who the beneficial owner(S) is /are.

11.7 Beneficial ownership

For opening an account of a Legal Person, who is not a natural person, the beneficial owner(s) should be identified and all reasonable steps in terms of sub rule (3) of Rule 9 of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 to verify his / her identity should be undertaken keeping in view the following:

Where the customer or the owner of the controlling interest is 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.

(a) Where **the client is a Company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person(s), has a controlling ownership interest or who exercises control through other means.

Explanation- For the purpose of this sub clause-

1. "Controlling ownership interest" means ownership of or entitlement to **more than 25%** of shares or capital or profits of the company;

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

(b) Where **the client is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of/entitlement to majority **more than 15%** of capital or profits of the partnership;

(c) Where **the client is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to **more than 15%** of the property or capital or profits of such association or body of individuals;

Explanation- Where no natural person is identified under (a) or (b) or (c) above, the Beneficial Owner is the relevant natural person who holds the position of the Senior Managing Official.

(d) Where **the client is a Trust**, the identification of beneficial owner(s) shall include identification of the author of the Trust, the Trustee, the Beneficiaries with **15% or more** interest in the Trust and any other natural person exercising ultimate effective control over the Trust through a chain of control or ownership; and the nature of the Trust or other arrangements in place should be obtained.

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

11.8. Trust / Nominee or Fiduciary Accounts

a. There exists the possibility that Trust / Nominee or Fiduciary Accounts can be used to circumvent the customer identification procedures. Bank will therefore examine and determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, bank will insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place.

b. While opening an account for a Trust, bank will take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories (Annexure- D). Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps will be taken to verify the founder managers/ directors and the beneficiaries, if defined.

➢ For opening an account of a Trust, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:
A certified copy of the latest entry in the public trust registers which shows the name of the trust, the Public Trust Register No. of the TRUST, at which it is registered and the name of the trustees.
a. Registration certificate,
b. Trust deed
c. Permanent Account Number(PAN) or Form No. 60 of the Trust
d. One copy of officially valid documents containing details of identity and address, one recent photograph and Permanent account number or FORM 60 of the person holding an attorney to transact on its behalf.

e. A resolution passed in a proper meeting held by all the trustees as to the opening of the account with a particular bank and the mode of operation of the account should be obtained.

The number of trustees to operate the account, should bear some reasonable proportion to the total number of trustees. If there are less than 4 to 5 trustees, 2 may be sufficient to operate the account. If number of trustees is larger, then the number of operating the account should be larger. The number should also have some relation to the amount allowed to be withdrawn either at a time or in total over a period of time.

Note: To open accounts in the names of trusts, executors, administrators, liquidator and HUF concerns, the branch should take permission of Regional Office.

11.9. Accounts of companies and firms

Bank will remain vigilant against business entities being used by individuals as a 'front' for maintaining accounts with bank. Bank will therefore examine the control structure of the entity, determine / ascertain the source of funds and identify the natural persons who have a controlling interest and who comprise the management. (Annexure – G)
For opening an account of a Company, certified copies of each of the following documents or equivalent e-documents thereof shall be obtained:

(a) Certificate of incorporation.

(b) Memorandum and Articles of Association

(c) Permanent Account Number of the Company

(d) A resolution from the Board of Directors and Power of Attorney granted to its Managers, Officers or Employees to transact on its behalf.

(e) One copy of officially valid documents containing details of identity and address, one recent photograph and Permanent account number or FORM 60 of the Managers, Officers or Employees, as case may be holding an attorney to transact on its behalf.

- In case of a public Ltd. company it will not be necessary to identify all the shareholders.

11.10. (A) Accounts of sole proprietary firms/concerns

For opening an account in the name of a sole proprietary firm, a certified copy of document containing details of identity and address of the individual (proprietor) as mentioned in Annexure-D should be obtained.

For proprietary concerns, in addition to the 'Officially Valid Documents' applicable to the individual (proprietor), **any two of the following documents or the equivalent e-documents thereof as a proof of business/activity** in the name of the proprietary concern are required to be submitted:

a. Registration certificate

b. Certificate/ license 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 License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.

g. Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.

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

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 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.

One copy of officially valid documents containing details of identity and address, recent photograph and Permanent account number or FORM 60 of the proprietor person.

Only documents mentioned in the above list are acceptable for opening of proprietorship accounts, as per extant guidelines of Reserve Bank of India. Therefore, Branches are advised to avoid accepting any other document for opening of proprietorship accounts.

It may also be noted that **Suchna Pavti /Intimation/Receipt of application for license under Shop and Establishment Act is not acceptable for opening of proprietorship accounts as** per extant guidelines of Reserve Bank of India. Only Certificate/license issued by the municipal authorities under Shop and Establishment Act is required to be obtained for this purpose.

It may be noted that **simplified measures guidelines** have been revoked by the Reserve Bank of India in latest Master Direction.

(B) Accounts of Partnership Firm

For opening an account of a partnership firm, the certified copies of each of the following documents shall be obtained:

(a) Registration certificate.

(b) Partnership deed.

(c) Permanent Account Number of the partnership firm

(d) One copy of officially valid documents containing details of identity and address, recent photograph and Permanent account number or FORM 60 of the person holding an attorney to transact on its behalf.

(e) Any of the following information to collectively establish the legal existence of such Partnership Firms

166.

- Certificate/ license issued by the municipal authorities under Shop & Establishment Act,
- CST / VAT/ GST certificates (provisional/ final)
- Certificate / registration document issued by Professional Tax authorities.
- IEC (Importer Exporter Code) issued by the office of DGFT/ License/ Certificate of Practice issued in the name of the concern by any professional body incorporated under a statute.
- The complete Income Tax return (not just the acknowledgement) in the name of concern where the income is reflected, duly Authenticated/ Acknowledged by the Income Tax Authorities.
- Utility bills such as electricity, water, and landline telephone bills in the name of the concerns.

(C)Accounts of an unincorporated association/Unregistered trusts or a body of individuals / Societies

For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents shall be obtained:

(a) Resolution of the managing body of such association or body of individuals.
(b) Permanent Account Number (PAN) **OR** Form 60 of the unincorporated association or a body of individuals
(c) Power of Attorney granted to the person to transact on its behalf;
(d) One copy of officially valid documents containing details of identity and address, recent photograph and Permanent account number or FORM 60 of the person holding an attorney to transact on its behalf and
(e) Any of the following information to collectively establish the legal existence of such an association or body of individuals:

- Certificate/ license issued by the municipal authorities under Shop & Establishment Act,
- CST / VAT/ GST certificates (provisional/ final)
- Certificate / registration document issued by Professional Tax authorities.
- IEC (Importer Exporter Code) issued by the office of DGFT/ License/ Certificate of Practice issued in the name of the concern by any professional body incorporated under a statute.
- The complete Income Tax return (not just the acknowledgement) in the name of concern where the income is reflected, duly Authenticated/ Acknowledged by the Income Tax Authorities.
- Utility bills such as electricity, water, and landline telephone bills in the name of the concerns.

Explanation: Unregistered trust shall be included under the term 'unincorporated association'.
Explanation: Term 'body of individuals' includes societies.

(D) Accounts of juridical persons such as Government or its Departments, Societies, universities and local bodies like Village Panchayats

For opening accounts of juridical persons not specifically covered in the earlier parts, such as Government or its Departments, Societies, Universities and local bodies like Village Panchayats, certified copies of the following documents or the equivalent e-documents shall be obtained:

(a) Document showing name of the person authorized to act on behalf of the entity;
(b) Aadhaar/ PAN/ Officially Valid Documents for proof of identity and address in respect of the person holding an attorney to transact on its behalf and;

167.

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

11.11 Periodical Updation of identification Data of Existing Customers:

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 as per the following procedure:

a. Branches will carry out-

- PAN verification from the verification facility available with the issuing authority and
- Authentication of Aadhaar Number already available with the Branch with the explicit consent of the customer, in applicable cases.
- In case, identification information available with Aadhaar does not contain current address, an OVD as per list given in Annexure-I containing current address may be obtained from the customer.
- Certified copy of OVD containing identity and address shall be obtained at the time of periodic updation from **individuals not eligible to obtain Aadhaar**, except from individuals who are categorized as 'Low Risk'. In case of Low Risk customers, when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.
- In case of Legal entities, Branch will review the documents sought at the time of opening of account and obtain fresh certified copies.

b. Branch 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., will be acceptable.

c.The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

d.In case of existing customers, Branches shall obtain Permanent Account Number (PAN) or equivalent e-document thereof, or Form No. 60 by such date as may be notified by the Central Government failing which, Branch shall temporarily cease operations in the account (in loan accounts, only credits to be allowed) till the time the Permanent Account Number or equivalent e-document thereof, or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing the operation in an Account, Branch shall give the customers an accessible notice and a reasonable opportunity to be heard. Those accounts, in which customer cannot submit PAN or equivalent e- document/Form No. 60 due to injury, illness or infirmity on old age or otherwise and such like causes, operation in the account to be continued with enhanced monitoring by Branches, which needs to be approved by appropriate authorities not below the rank of Regional Manager/Chief Manager (Co-Ordination).

If a customer gives in writing that she/he does not want to submit her/his Permanent Account Number or equivalent e-document or Form No. 60, Branch 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 RE 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.

12. Small Accounts

If an individual customer who does not have Aadhaar/enrolment number and PAN and desires to open a bank account, then **'Small Account'** may be opened for such an individual.

A "Small Account" means a Savings Account in which –

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

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

Further, small accounts are subject to the following conditions:

a) An individual who desires to open a "small account" may be allowed to open such an account on production of a self-attested photograph from the customer and affixation of signature or thumb print on the form for opening the account.

b) The designated officer (i.e. Branch Head or any other senior officer authorized by him) while opening the "small account", certifies under his signature that the person opening the "small account" has affixed his signature or thumb print, as the case may be, in his presence;

Provided that where the individual is a prisoner in a jail, the signature or thumb print shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature and the account shall remain operational on annual submission of certificate of proof of address issued by the officer in-charge of the jail.

c) Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account.

d) Branches to ensure that the stipulated limits on monthly and annual limits of aggregate of transactions and balance requirements in such accounts are not breached before a transaction is allowed to take place.

e) The account shall remain operational initially for a period of **twelvemonths**, which can be extended for a further period of **twelve months**, if the holder of such an account provides evidence before branch, of having applied for any of the officially valid documents during the first twelve months of the opening of the said account.

f) The entire relaxation provisions to be reviewed in respect of the said account after **twenty four months.**

g) Notwithstanding anything contained in clause (e) and (f) above, the small account shall remain operational between April1,2020 and June 30, 2020 and such other periods as may be notified by the central Government.

h) The small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of client shall be established as per section 16.

i) Foreign remittance shall not be allowed to be credited in to a **'small account'** unless the identity of the client is fully established through the production of "Officially Valid Documents" as per **Annexure D.** i.e. the account is converted to normal category.

Branches should take a note that "Small Accounts can be converted to PMJDY accounts by carrying out e-KYC/ KYC procedures on such customers. When such account holders come forward to use these accounts by way of deposit and/or withdrawal, steps should be taken by the Branches to carry out e-KYC/KYC exercise and simultaneously seed the accounts with their Aadhaar and mobile number, as appropriate.

Branches are, therefore, advised to take necessary steps to convert the Small Accounts to PMJDY accounts after taking necessary steps as mentioned above. If any account is rendered ineligible for being classified as a small account due to credits/ balance in the account exceeding the permissible limits, withdrawals may be allowed within the limit prescribed for small accounts where the limits thereof have not been breached yet.

(j) Branches are not required to obtain fresh documents from customers when they approach for transferring their account from one branch to another branch.
Branches are advised to note that KYC verification done by one Branch of our Bank is valid for transfer of account within the Bank if full KYC verification has been done for the concerned account and is not due for periodic updation.

(k) Further, if an existing KYC compliant customer desires to open another account with our Bank, she/he need not submit fresh proof of identity and/or address. There is no need for a fresh CDD exercise.

13. Monitoring of Transactions

"Ongoing Due Diligence" means regular monitoring of transactions in Customer's accounts to ensure that they are consistent with the customers' Business, risk profile and source of funds. Ongoing monitoring is an essential element of effective KYC procedures. Bank can effectively control and reduce its risk only if it has an understanding of the normal and reasonable activity of the customer so that it has the means of identifying transactions that fall outside the regular pattern of activity.

However, the extent of monitoring will depend on the **risk category** of the account. i.e. High Risk accounts have to be subjected to more intensify monitoring.

- **Bank will pay special attention to all the following types of transactions:**

i. 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.

i.

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

iii.Transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer.

iv.High account turnover inconsistent with the size of the balance maintained.

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

Note: High Risk accounts have to be subjected to more intensified monitoring.

Bank has put a system of risk categorization of the customers at the time of the opening the accounts. Further, there is a system of periodical review of risk categorization of the customers which is carried out every six months i.e. in March and September every year. Branches are provided with the data through CBS system for applying enhanced due diligence for High Risk customers.

Bank has prescribed / defined various threshold limits for transactions in accounts of individuals and non-individuals in its AML Solution which will generate Alerts for detection of suspicious transactions and thereby monitoring transactions in the accounts. This will enable bank to pay particular attention to the transactions which exceed these limits.

Bank has installed a software to generate transaction based AML Alerts when they breach the thresholds fixed for different types of customer's accounts. The alert definitions are predefined as per the Alert Indicators advised by Working Group of IBA. Further, Bank has established the AML Department at Head Office, Ajmer to monitor the transaction based alerts, detect the suspicious transactions and to escalate the unusual transactions to the Principal Officer for submission of STR in appropriate cases.

➢ **Transaction monitoring (Alerts generated though AML Software)**

Bank is using different scenarios to identify "Suspicious Transaction" for reporting of the STRs to Financial Intelligence Unit, Government of India (FIU-IND). In July 2010, Ministry of Finance, under Govt. of India felt the need to form a "Working Group" consisting representatives from selective banks, RBI, IBA and FIU-IND to evolve standard parameters for generation of suspicious transaction alerts. Accordingly a list of commonly used -61- alert indicators for detection of suspicious transactions was provided by IBA (enclosed in Annexure – F-5 Part - II). These alert indicators were related to following sources:-

- Watch list (WL) – The customer details matched with watch lists (e.g. UN list, Interpol list etc.)
- Transaction monitoring (TM) – Transaction monitoring alert (e.g. unusually large transaction, increase in transaction volume etc.)
- Typology (TY) – Common typologies of money laundering, financing of terrorism or other crimes (e.g. Structuring of cash deposits etc.)
- Risk Management System (RM) – Risk management system based alert (e.g. high risk customer, country, location, source of funds, transaction type etc.)

➢ **Review of Alert Definitions predefined in Financial Crime Detection and Management System (FCDMS PROGRAMME)**

Bank will review the thresholds and frequencies predefined in the existing alert definitions in the FCDMS system periodically. It would be implemented only after getting approvals from the competent authorities. Bank's Internal Accounts should not be excluded from AML screening.

The exercise should take place at Regular Intervals preferably on an annual basis. The Audit of the system will be done by the IS Audit Department.

➢ **Data Purging/ Archiving of Old Data available in Financial Crime Detection and Management System (FCDMS)**

As there is a government requirement under PMLA that information must be kept for 5 years, Bank must be able to retrieve archived information on request, whenever required.

➢ **Behavioral Transaction Monitoring**

There are certain types of transactions which can be identified at the branch themselves. The identification of such suspicious transactions is more likely to be related with following sources.

- Customer verification (CV): Detected during customer acceptance, identification or verification (e.g. Use of forged ID, wrong address etc.)
- Law Enforcement Agency Query (LQ): Query or letter received from law enforcement agency (LEA) or intelligence agency (e.g. blocking order received, transaction details sought etc.)
- Media Reports (MR): Adverse media reports about customer. (e.g. newspaper reports)
- Employee Initiated (EI): Employee raised alert (e.g. behavioral indicators such as customer had no information about transaction, attempted transaction etc.)
- Public Complaint (PC): Complaint received from public (e.g. abuse of account for committing fraud etc.)
- Business Associates (BA): Information received from other institutions, subsidiaries or business associates (e.g. cross-border referral, alert rose by agent etc.)

The list of -27- commonly used behavioral alert indicators for detection of suspicious transactions at branches is given in (Annexure – F-5 Part – I).

In order to fulfill obligations under PMLA, 2002, Bank has to report these suspicious transactions to FIU-IND. Branches are advised to report such identified/ attempted transactions by generating the alert through CBS Menu 'AMLALERT' by providing detail of the incident. The alert will be displayed in the list of AML alerts of the AML CELL for onward submission of STRs to Principal Officer at Head Office, Ajmer in order to review the case for reporting of STR.

All the field functionaries/ branch staff are required to be vigilant to detect and report such offline alerts. Detailed list of such behavioral alert scenarios along with the Job Card of Menu 'AMLALERT' has been forwarded to the branches/ offices shortly on activation of menu "AMLALERT" in FINACLE system.
Branches have been advised to escalate suspicious behavior through CBS Menu "AMLALERT" if they notice any of the -27- suspicious behaviors of the customers during the Branch operations.

Branches are also advised to contact their respective Regional office for their guidance while deciding on reporting of behavioral alerts. The Regions are advised to effectively monitor and guide the branches in reporting of such behavioral alerts through CBS Menu 'AMLALERT' and further filing of the STRs to the Principal Officer in the electronic format as prescribed by the FIU-IND.

Role of branch officials in reporting behavioral alerts for identifying suspicious transactions is very important. Dealing officer/employee in the front desk should be well aware of such identified/ attempted transactions which could not be captured by the system. As such all field functionaries are required to be vigilant and keep themselves aware of the alert indicators and indicative suspicious activities, an indicative list of suspicious activities is provided in Para 22.2(9) (Page No. 55)

➢ **Trade Based Money Laundering (TBML)**

With a view to strengthen the process of identification of possible suspected/ non genuine trade transactions at the transaction level, FIU-IND working group on TBML has identified -63- Red Flag Indicators (RFIs). The list of Red Flag Indicators (RFIs) defined for identifying the suspicious transactions related to TBML is attached in Annexure – I of this Policy.

Branches are advised to use the RFIs at the transaction level for all trade transactions and report all such suspicious/ non trade transactions to respective Regional Office. Regional Offices are advised to properly analyze such cases and the case should be brought to the notice of Principal Officer for filing of STRs to FIU-IND. It should be ensured that the above analysis process should not lead to tipping off to the customer.

Further, Bank is in process to define alert definitions on these Red Flag Indicators (RFIs) for generation of alerts on detection of predefined patterns in potentially suspicious Trade Based Money Laundering (TBML) Transactions.

➢ **ANTI MONEY LAUDERING CELL (AML CELL)**

AML CELL will ensure compliance in respect of the handling of AML Alerts, filing of STR and CTR and Roles/ Responsibilities mentioned as under.

- **Role and Responsibilities of AML CELL**:

AML CELL generates alerts on various parameters in Financial Crime Detection Management system software named as: AMLOCK. AMLOCK has 3 layer user architecture. L1 and L2 users are at Regional office level and L3 user at Head office level for scrutiny of generated alerts.
AML Cell generates alerts based different parameters through AMLOCK software on fortnightly basis in connection with transaction taking place in accounts at branches. Generated alerts assigned to L1 users respectively.

a. Thorough scrutiny/process of alerts generated on transaction taken place in branch is done by AMLOCK user on the basis of customer profile information available in finacle system.

b. To verify the nature of transactions on the basis of alerts generated in the respective accounts, with proper due diligence.

c. Follow up with the L1/L2 user for closure or further process of alerts to avoid delay in identification of suspicious alerts if any.

d. Assignment of generated alert to higher level user(L2/L3) if any suspiciousness found in generated alert by current user(L1/L2) to report the same to competent authority for file STR to FIU IND.

e. To ensure marking of Trusted accounts in the AMLOCK (for non-generation of alerts in next three months under that category), if on scrutiny transaction taken place in account on which alert generated is as per customer profile.

f. AML Cell will make sure to mark the account to high risk for which STR filed in FIU-INDIA.

g. Reporting of CTRs: Data Center will generate CTRs for all branches through AMLOCK system. Thereafter, At Head Office, AML CELL will validate the xml file through FIU-IND Software and generate Hash file digitally signed by Principal Officer, which is further uploaded to Fin-net portal of FIU- IND on or before 15th of the succeeding month.

h. Review of Alert Definitions: To review the thresholds and frequencies predefined in the existing alert definitions in the FCDMS system periodically.

i. Reporting of STRs: Prepare STRs from the AML Alerts generated by the AML Software and Behavioral Alerts generated by the branches from suspicious angle and report STRs to Principal Officer (PO) within seven days from the date of arriving at a conclusion that transaction is suspicious one.

- Bank will exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with bank's knowledge of the client, his business and risk profile and wherever necessary, the source of funds.

- High and Medium Risk Categorized accounts will be subjected to intensify monitoring. For the purpose, bank will consider background of the customer, i.e. country of origin, sources of funds, the type of transactions involved and other risk factors. High risk associated accounts of bullion dealers (including sub-dealers) and jewelers to be taken into account by the bank to identify the suspicious transactions for filing Suspicious Transaction Reports (STRs) to FIU-IND.

Accounts in which suspicious transactions are reported will be classified as High Risk and also be subjected to further monitoring.

The risk categorization of customers as also compilation and periodic updation of customer profiles, monitoring and closure of alerts in accounts by Bank is extremely important for effective implementation of KYC/AML/CFT measures. Bank will, therefore, ensure compliance with the regulatory guidelines on KYC-AML-CFT both in letter and spirit by the process of risk categorization and compiling / updating profiles of existing customers and monitoring and closure of alerts in accounts.

Bank has put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorization of customers will be carried out at a periodicity of not less than once in six months.

➢ **White-listing/ Trusted Accounts for AML System**

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

The accounts for white-listing/ Trusted Accounts should be screened by the Regional Offices in consultation with the respective branch wherein the account is held by the customer keeping records at the Regional Office for future reference while Audit/ Inspection by the RBI / NABARD Officials/ Concurrent Auditors. All such trusted accounts are to be verified and recommended by the Regional Head/ Deputy Regional

Head for 'white listing' or marking it as trusted under his/her signature by giving proper reason in each case maintaining top secrecy.

White-listing of accounts should not be applicable for impersonal accounts like Sundry Creditors etc. which are prone to operational risk through fraudulent means. Therefore, AML Team at Region should monitor such accounts to avoid unnecessary routing of transactions through it.

➢ **Multi-level Marketing (MLM) companies**

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

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

Caution is to be exercised in opening accounts of the MLM firms and issue of cheque books in such accounts. Also strict compliance of KYC and AML guidelines and Cheque issue guidelines should be ensured.

The names of some of the firms provided by RBI were circulated to the branches (Annexure- H) for exercising caution while opening and operating the accounts of such firms. RBI has noticed that such Companies/ Individuals have been identified/ suspected of carrying out MLM activities.

Branches are advised to be cautious in opening and operating accounts for such schemes especially in view of the type of business and inherent risk associated with such activity.

➢ **Money Laundering and Terrorist Financing Risk Assessment by Bank:**

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

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

(b) The risk assessment by the Bank shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Bank. Further, the periodicity of risk assessment exercise shall be determined by the Board of the

Bank, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.
(c) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated, and should be available to competent authorities and self-regulating bodies.

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

14. Risk Management

As banks are exposed to various risks (i.e. reputation risk, compliance risk, operational risk, concentration risk, legal risk etc.) which may arise out of Money Laundering Malpractices by its customers, Bank will exercise on-going due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with bank's knowledge of the client, his business and risk profile and wherever necessary the source of funds.

The Audit Committee of the Board (ACB) ensures that an effective KYC programme is put in place by establishing appropriate procedures. It also ensures that KYC programme is effectively implemented at all levels in the Bank. For the purpose, the Bank has allocated explicit responsibility to various authorities within the Bank for ensuring effective implementations of Bank's KYC policy guidelines and procedures.

From time to time, Bank will, in consultation with Audit Committee of Board, devise procedures for creating risk profiles of existing and new customers, assess the risk in dealing with various countries, geographical areas and also the risk of various products, services, transactions, delivery channels, etc. Bank has prescribed policies and procedures to effectively manage and mitigate these risks adopting a risk based approach.(Annexure-F & Annexure F-1 to Annexure F-5 part I &II)

Customers should be classified as Low, Medium and High Risk category, based on the assessment and risk perception by them.

Branches are, therefore, advised to assign proper Risk Category to the new customers at the time of on-boarding as well as at the time of periodic KYC updation, based on parameters such as customer's identity, social/financial status, nature of business activity, information about the clients' business, their location and transactions etc. Branches have to enter correct constitution code in Finacle to enable the system to assign proper Risk category to the accounts automatically.

While considering customer's identity, the exercise to confirm identity documents through online or other services offered by issuing authorities may also be carried on. Branches are also advised to invariably mark the risk category in Account Opening Form at proper space provided.

As a general rule, the compliance function will provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Bank's internal inspection, audit and compliance functions will therefore play and/or have an important role in evaluating and ensuring adherence to the KYC-AML-CFT Policy and procedures.

Internal Inspectors and Concurrent Auditors will specifically check and verify the application of KYC procedures at the branches in newly opened accounts as well as in the existing accounts and will comment on the lapses observed in this regard. Bank will ensure that its audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Compliance function will give feedback to Principal Officer based on inspection reports for necessary action.

The compliance in this regard will be put up to the Board at regular intervals.

15.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 Bank 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. Marketing of credit cards shall also be subjected to due diligence and KYC measures.

16. Combating Financing of Terrorism (CFT)

In terms of PMLA Rules, suspicious transaction should include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism.

Bank will therefore ensure for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suspicious transaction reports to the Financial Intelligence Unit India (FIU-IND) on priority.

As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank of India circulates these to all banks.

17. Watch list Alerts (WL):

Bank has developed software for on-line list matching of names of customer with the banned / black lists as a measure of abundant precaution to avoid human interference and /or error in checking the list manually. The updation of all such lists in the on-line list matching software is done at Data Center level whenever any new updates in the list are notified by the Reserve Bank of India. The System will throw Watch list alerts for such instances where the name of account holder matches with the banned / black list entities/ individuals. The system throws warnings to the branch users in case the customer's name matches with any individual / entity of the 'Sanctions Lists'. Branches have been advised to ensure that they do not open accounts of the individuals / entities appearing in the above lists and does not permit to verify the Customer ID. Under such situation, branch users should recheck the identity of the customer and again verify in the system. Bank will carry out Client Due Diligence before examining/ investigating/ closing the Watch list alerts and file the STRs, if found suspicious.

18.Requirements/obligations under International Agreements:

The UN Security Council has adopted resolutions 1988 (2011) and 1989(2011) which have resulted in splitting of the 1267 Committee's Consolidated List into two separate lists, namely:

(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.

Both "ISIL (Da'esh) & Al-Qaida Sanctions List" and "1988 Sanctions List" are to be taken into account for the purpose of implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967.

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 February 2,2021 (**Annex.- C**- Annex II of RBI Master Direction **RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 Dated February 25, 2016 (Updated as on May 10, 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.

19. Freezing of financial assets

The procedure laid down in the UAPA Order dated February 2,2021 (Annex II of RBI Master Direction **RBI/DBR/2015-16/18 Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 Dated February 25, 2016 (Updated as on May 10, 2021)** shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

20.Designated Director and Principal Officer (PO)

20.1 Designated Director

Bank has nominated the Chairman of the Bank as "Designated Director", as required under the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Rules), to ensure overall compliance with the obligations under the Act and Rules.

20.2 Principal Officer (PO)

Under PMLA, 2002, Bank is required to appoint Principal Officer for reporting of prescribed transactions. Bank has appointed / designated General Manager of the Bank as Principal Officer (PO) who will act independently and report directly to the Board of Directors and will be located / stationed at the Head office of the bank.

20.2.1. Responsibilities of Principal Officer:

Principal Officer will be responsible for

a. Implementation of the bank's KYC-AML-CFT Policy in the bank.

b. Sharing of information as required under the law.

c. Maintaining close liaison with enforcement agencies, banks and any other institution which are involved in the fight against Money Laundering and Combating Financing of Terrorism (CFT)

d. Ensuring submission of cash Transaction Report (CTR) to FIU-IND, New Delhi within 15 days of every succeeding month.

e. Ensuring submission of Suspicious Transaction Report (STR) to FIU-IND, New Delhi within seven days from the date of arriving at conclusion that transaction is suspicious.

f. Ensuring submission of Counterfeit Currency Report (CCR) to FIU-IND, New Delhi by 15th of the succeeding month.

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

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

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

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

20.2.2. Assistance / support to the Principal Officer:

The Chief Manager (CBS & IT) will lend all necessary technological support for acquisition, establishment and maintenance of AML Solution / software and hardware requirement of KYC-AML Department at Head Office and also improvement/ modification in existing software/ utilities and up gradation of hardware from its vendors/ system integrators from time to time as per requirement of the Principal officer.

Data Center will assist by submitting CTRs/ NTRs/ EFTs of all the branches in electronic format to Principal Officer within 4 days of succeeding month. Data Center will also assist by running utility for branches to review Money Laundering Risk Categorization in December and June every year and send its confirmation to Principal Officer.

Principal Officer will be assisted by Chief Compliance Officer of Compliance Department headed by Senior Manager for compliance of Bank as a whole. Bank will ensure that the necessary infrastructure and staff component is provided to KYC-AML Department at Head Office as deemed fit and necessary by Principal Officer (PO) for its efficient functioning.

a. Branches are under close supervision of their Regional Authorities

b. Primarily branches have to implement KYC-AML-CFT policy of the bank as transactions take place at branches and to be monitored by them.

20.3. Responsibilities of Regional Heads:

Regional Heads will:

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

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

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

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

e. Training : Training will be arranged by HRM Department for one/two days seminars/ workshops on KYC-AML-CFT guidelines at their office / training centers with the help of faculty members of training centers for spreading awareness amongst frontline staff in their branches.

20.4. Responsibilities of Chief Manager at RO :

Deputy Regional Manager will -

a. Ensure 100% compliance of KYC-AML-CFT guidelines in newly opened accounts and in all existing accounts by their branches.

b. Ensure to submit confirmation for 100% compliance of bank's KYC-AML-CFT policy guidelines by their branches in all existing accounts to Principal Officer (PO) on half yearly basis in the first week of January and July every year.

c. Ensure that branches invariably update customer identification data (including photo) once in **Ten Years** after account is opened in case of Low Risk Customers and **once in two years** after account is opened in case of High **and once in eight years** for Medium Risk Customers to meet with the Regulatory requirements.

d. Counterfeit Currency Reports (CCRs): Ensure that branches invariably report to nodal officer in case of detection of fake / forged currencies. Also ensure for prompt reporting of CCRs by branches to their office and in turn will ensure to submit CCRs to Forged Note Vigilance Cell under Operation Department at the Head Office of the Bank as per circular no. HO:OPR-10/06/143 Dtd. 16.07.2018 on the same day of reporting of CCRs by branches.

e. Money Laundering Risk Categorization: Ensure that all the branches under their control strictly observe bank's guidelines in respect of Money Laundering Risk Categorization (MLRC) while opening new account and also of existing accounts and review existing Risk Categorization at stipulated intervals i.e. in March and September every year.

f. Monitoring of Transactions: Ensure that branches monitor high value transaction, transactions in newly opened accounts for the initial six months, transactions in High / Medium Risk Accounts and transactions in accounts where STRs are reported to FIU-IND.

20.5. Responsibilities of Staff at Branches:

All the staff members who are associated with account opening, interact with the customer and or process/handle their transactions, whether cash, transfer or clearing, will be responsible for scanning/examination of transactions from money laundering risk

perception/angle and bring immediately to the notice of their Branch Head any suspicious transaction / activity of customer observed by them and advice AML CELL for filing STRs.

All the staff members, who are associated with account opening, should ensure that all the fields of the account opening form are duly filled in and proper risk category has been assigned to the respective customer based of his/ her profile. It is advised the branch to do due diligence and ensure to update latest KYC profile of the customer like constitution code, occupation code etc. in the system and do not fill **"Others" and left blank** any field while updating customer details in system.

All the staff members must remain vigilant about the customer behavior in the branch and generate behavioral alerts through Menu "AMLALERT" in CBS, if any suspicious behavior is noticed, on the basis of -27- behavioral alert indicators provided by the IBA.

Any lapse and intentional circumvention on prescribed procedure and guidelines contained in KYC-AML-CFT policy of the bank by any of the staff will be viewed seriously and necessary action will be taken as deemed fit by bank.

20.6. Other Roles and Responsibilities of Bank Officers/ Employees

Bank officers/ employees will conduct themselves in accordance with the highest ethical standards and in accordance with the extant regulatory requirements and laws. They should not knowingly provide advice or other assistance to individuals who are indulging in laundering activities.

Bank officers/employees who suspect money-laundering activities should refer the matter to appropriate authority.

Bank officers/employees should not indulge in unnecessary dialogue or provide unwanted guidance to the customers / intended customers to avoid dispute of any kind in future.

Failure to adhere to KYC / Money Laundering policies / procedures may subject bank employees to appropriate disciplinary action or such penal actions and penalties that may be stipulated under any law or regulatory directive.

In general terms there are **FIVE** golden rules to be followed:

1. You **MUST NOT** assist anyone whom you know or suspect to be laundering money that has been derived from any serious crime.
2. You **MUST** report any transaction which you suspect might be related to drugs, terrorism or other serious crimes.
3. You **MUST NOT** reveal in any way to anyone that a customer is being investigated or that they have been the subject of a report except your Branch Manager and controlling authorities.
4. You **MUST NOT** go overboard in seeking information for KYC compliance and thereby invading into client's privacy.
5. You **MUST NOT** divulge customer information for cross selling or any other like purposes.

20.2.7. Responsibilities of Branch Heads:

a. Reporting of Counterfeit Currency (CCRs) to their Regional Head as per Circular no.HO:OPR-10/06/143 Dtd. 16.07.2018 in the format prescribed by FIU-IND on detection any counterfeit currency notes. These cash transactions will also include transactions where

forgery of valuable security or documents has taken place and will be reported in the form as prescribed by bank to FIU-IND.

b. Examination / monitoring of High Value Cash Transaction (CTRs / NTRs) from suspicious angle and report the same to the respective Regional Head, if found suspicious **and keep a verifiable records of CTRs/ NTRs in the branch itself.**

c. Monitoring of transactions in newly opened accounts as well as accounts categorized as High / Medium Risk.

d. Ensuring 100% compliance of KYC-AML-CFT policy guidelines of the bank while opening new accounts as well in existing accounts.

e. Sending confirmation on Monthly basis to their Regional Authorities for having complied fully with the KYC-AML-CFT guidelines of the bank in new as well old existing accounts in the first week of succeeding month.

f. Branches need to continue to carry out on-going due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and, wherever necessary, the source of funds.

Full KYC exercise will be required to be done at least every **two years** for high risk individuals and entities.
Full KYC exercise will be required to be done at least every **ten years** for low risk and at least every **eight years** for medium risk individuals and entities.

Positive confirmation (obtaining KYC related updates through e-mail/ letter/ telephonic conversation/ forms/ interviews/ visits etc.), will be required to be completed at least every two years for medium risk and at least every three years for low risk individuals and entities.

Fresh photographs will be required to be obtained from minor customer on becoming major and that time it shall be ensured that CDD documents as per the current CDD standards are available. Wherever required, branch/bank may carry out fresh KYC of such customers.

g. Ensuring Money Laundering Risk Categorization of new customer while opening the account as well of all the existing customers of the branch and generating report thereof and preserving the same for inspection by Internal Inspectors / Concurrent Auditors / Reserve Bank of India.

h. Ensuring review of Money Laundering Risk Categorization twice in a year i.e. in December and June every year and sending confirmation thereof in the first week of the January and July to their Regional Authorities to meet with the requirement of Regulators.

i. Maintenance of records of prescribed transactions, verification of identity of customers and documents thereof as prescribed in PML ACT 2002 and mentioned hereafter in this policy document.

j. Ensuring immediate rectification of deficiencies in KYC Documents if any observed by internal inspectors / Concurrent Auditors / NABARD during inspection of the branch.

21. Prevention of Money Laundering (PML) Act, 2002.

Government of India, Ministry of Finance, Department of Revenue, vide its notification dated July 1, 2005 in the Gazette of India, has notified the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the said Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005.

21.1. Definition of Money Laundering under PML Act, 2002

Section 3 of the Prevention of Money Laundering (PML) Act, 2002 has defined the "offence of money laundering" as under:

"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".

Money launderers use the banking system for cleansing 'dirty money 'obtained from criminal activities with the objective of hiding / disguising its source.

The process of money laundering involves creating a web of financial transactions so as to hide the origin and true nature of these funds.

For the purpose of this document, the term 'money laundering' would also cover financial transactions where the end use of funds goes for financing terrorist irrespective of the source of the funds.

21.2. Punishment for Money Laundering:

Section 4 of the Prevention of Money Laundering Act, 2002 specifies punishment for Money Laundering as under:

"Whoever commits the offence of Money Laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to seven years and shall also be liable to fine which may extend to five lakh rupees."

Provided that where the proceeds of crime involved in money-laundering relates to any offence specified under paragraph 2 of Part A of the Schedule, the provisions of this section shall have effect as if for the words "which may extend to seven years", the words "which may extend to ten years" had been substituted.

21.3 Obligation of banks under PML Act, 2002.

Section 12 of the PMLA, 2002 casts certain obligations on the banks in regard to preservation and reporting of customer account information which include:

a. Maintaining a record of prescribed transactions

b. Furnishing information of prescribed transactions to the specified Authority

c. Verifying and maintaining records of the identity of its clients

d. Preserving records in respect of (a), (b), above for a period of **5 years** from the date of transaction and (c) above from the date of cessation of transaction with the client.

21.4. Record Management

Maintenance of records of transactions

Bank will adopt / introduce a system for maintaining proper record of all transactions including record of transactions prescribed under Rule 3, as mentioned below:

a. All cash transactions of the value of more than Rupees Ten Lakh;

b. All series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakh or its equivalent in foreign currency where such series of transactions

have taken place within a month and the aggregate value of such transactions exceed Rupees Ten Lakh;

c. All cash transactions where the forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transaction;

d. All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

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

(a) Maintain all necessary records of transactions between the Bank and the customer, both domestic and international, **for at least five years from the date of transaction**;

(b) Preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, **for at least five years after the business relationship is ended**;

(c) Make available the identification records and transaction data to the competent authorities upon request;

(d) Introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);

(e) Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

(i) the nature of the transactions;

(ii) the amount of the transaction and the currency in which it was denominated;

(iii) the date on which the transaction was conducted; and

(iv) the parties to the transaction.

(f) Evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities;

(g) Maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

21.5. Powers of Director (Financial Intelligence Unit) to impose fine:

As per Section 13, if the Director, in the course of any inquiry, finds that bank or any of its officers has failed to comply with the provisions contained in Section 12, then, without prejudice to any other action that may be taken under any other provisions of PML Act, he may by an order, levy a fine on bank which shall not be less than Ten Thousand Rupees but may extend to One Lakh Rupees for each failure.

Furnishing of Information to the Director (FIU-IND)

In terms of new addition to rule 8(4), while furnishing of information to the Director FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying

mis- represented transaction beyond the time limit as specified in the rule shall constitute 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.

21.6. No Civil Proceeding against Bank and its Officers.

As per Section 14, the bank and its officers shall not be liable to any civil proceedings against them for furnishing information under clause (b) of sub-section 12.

22. Reports to be furnished to FIU-IND

Bank follows the detailed guidelines contained on compilation and manner / procedure of submission of following reports prescribed by FIU-IND and ensure for its error free and timely submission to them.

a. Cash Transactions Report (CTR)
b. Suspicious Transactions Report (STR);
c. Counterfeit Currency Report (CCR);
d. Non Profit Organizations Transactions Report (NTR)
e. Cross-Border Wire Transfer Report (EFT)

22.1Cash Transaction Reports (CTRs):

Bank will file following types of Cash Transactions to FIU-IND, New Delhi.

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

Explanation –

Integrally connected cash transactions referred to at (b) above. The following transactions have taken place in a branch during the month of April, 2008:

Date	Mode	Dr. (in ₹)	Cr. (in ₹)	Balance
Balance BF				8,00,000.00
02/04/2008	Cash	5,00,000.00	3,00,000.00	6,00,000.00
07/04/2008	Cash	40,000.00	2,00,000.00	7,60,000.00
08/04/2008	Cash	4,70,000.00	1,00,000.00	3,90,000.00
Monthly Summation		**10,10,000.00**	**6,00,000.00**	

As per above clarification, the debit transactions in the above example are integrally connected cash transactions because total cash debits during the calendar month exceeds Rs10 lakhs.

All the credit transactions in the above example would not be treated as integrally connected, as the sum total of the credit transactions during the month does not exceed ₹ 10 lakh and hence credit transaction dated 02, 07 & 08/04/2008 should not be reported by banks.

➢ While filing CTRs, details of individual transactions below Rupees Fifty Thousand will not be furnished.

➢ CTRs will contain only the transactions carried out by the bank on behalf of their clients/ customers excluding transactions between the internal accounts of the bank.

➢ **Data Center will generate CTRs for all branches through the AMLOCK system in XML file format. Head office convert edit to Hash files, digitally signed by Principal Officer, which is further uploaded to Fin-net portal of FIU- IND on or before 15th of the succeeding month.**

22.2 Suspicious Transaction Reports (STR)

Bank will file all suspicious transactions as mentioned in the PMLA Rules to Financial Intelligence Unit – India (FIU-IND). While determining suspicious transactions, bank will be guided by definition of suspicious transaction contained in PMLA Rules as amended from time to time. Bank also files Suspicious Transaction Reports (STR) to FIU-IND for Mobile Banking Transactions as in case of normal banking transactions.

Definition of Suspicious Transaction in PMLA Rules:

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

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

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

c. Appears to have no economic rationale or bonafide purpose; or

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

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

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

➢ **Bank will make STRs if it has reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged to predict offences.**

➢ **As a part of transaction monitoring mechanism, Bank has procured Financial Crime and Detection and Management System (FCDMS) Software to throw AML alerts when the transactions are inconsistent with risk categorization and updated profile of the customer. It is essential for effective identification and reporting of suspicious transaction.**

In the context of creating KYC-AML awareness among the staff and for generating alerts for suspicious transactions, bank will consider the indicative list of suspicious activities contained in the IBA's Guidance Note for Banks, January 2012 are given below.

➢ **An Indicative List of Suspicious Activities:**

(1) Transactions Involving Large Amounts of Cash

a. Exchanging an unusually large amount of small denomination notes for those of higher denomination;

b. Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;

c. Frequent withdrawal of large amounts by means of cheques, electronic fund transfers;

d. Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;

e. Large cash withdrawals from a previously dormant/inactive/inoperative account, or from an account which has just received an unexpected large credit from abroad;

f. Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company, e.g. cheques, letters of credit, electronic fund transfers etc.;

g. Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.

(2) Transactions that do not make Economic Sense

a. A customer having a large number of accounts with the same bank, with frequent transfers of funds between different accounts;

b. Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.

(3) Activities not consistent with the Customer's Business

a. Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.

b. Corporate accounts where deposits & withdrawals by cheque/ foreign inward remittances/ any other means are received from/ made to sources apparently unconnected with the corporate business activity/dealings.

c. Unusual applications for DD against cash.

d. Accounts with large volume of credits through DD whereas the nature of business does not justify such credits.

e. Retail deposit of many cheques but rare withdrawals for daily operations.

(4) Attempts to avoid Reporting/ Record-keeping Requirements

a. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.

b. Any individual or group that coerces/ induces or attempts to coerce/ induce the bank employee not to file any reports or any other forms.

c. An account where **there are several cash deposits/ withdrawals below a specified threshold** level to avoid filing of reports that may be necessary in case of transactions above the

threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

(5) Unusual Activities

a. An account of a customer who does not reside/ have office near the branch even though there are bank branches near his residence/ office.

b. A customer who often visits the safe deposit lockers immediately before making cash deposits, especially deposits just under the threshold level.

c. Funds coming from the list of countries/ centers which are known for money laundering.

(6) Customer who provides Insufficient or Suspicious Information

a. A customer/ company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors, or its locations.

b. A customer/ company who is reluctant to reveal details about its activities or to provide financial statements.

c. A customer who has no record of past or present employment but makes frequent large transactions.

(7) Certain Suspicious Funds Transfer Activities

a. Sending or receiving frequent or large volumes of remittances to/from countries outside India.

b. Receiving large DD remittances from various centers and remitting the consolidated amount to a different account/Centre on the same day leaving minimum balance in the account.

c. Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire/ funds transfer.

(8) Certain Bank Employees arousing Suspicion

a. An employee whose lavish lifestyle cannot be supported by his or her salary.

b. Negligence of employees/ willful blindness is reported repeatedly.

(9) List of alert Indicators of suspicious activities/transactions to be monitored by the operating staff at Branch Level-

Sr.no.	Alert Indicator	Indicative Suspicion
1.	Customer left without opening account	Customer did not open account after being informed about KYC requirements.
2.	Customer offered false or forged identification documents	Customer gives false identification documents or documents that appear to be counterfeit, altered or inaccurate.
3.	Identity documents are not verifiable	Identity documents presented are not verifiable i.e. Foreign documents etc.
4.	Address found to be non-existent	Address provided by the customer is found to be non-existent
5.	Address found to be wrong	Customer not staying at the address provided during account opening
6.	Difficult to identify beneficial owner	Customer uses complex legal structures or where it is difficult to identify the beneficial owner
7.	Customer is being investigated	Customer has been the subject of inquiry from

	for criminal offences	any law enforcement agency relating to criminal offences
8.	Customer is being investigated for TF offences	Customer has been the subject of inquiry from any law enforcement agency relating to TF or terrorist activities
9.	Adverse media report about criminal activities of customer	Match of customer details with persons reported in local media / open source for criminal offences
10.	Adverse media report about TF or terrorist activities of customer	Match of customer details with persons reported in local media / open source for terrorism or terrorist financing related activities
11.	Customer did not complete transaction	Customer did not complete transaction after queries such as source of funds etc.
12.	Customer is nervous	Customer is hurried or nervous
13.	Customer is over cautious	Customer is over cautious in explaining genuineness of the transaction.
14.	Customer provides inconsistent information	Customer changes the information provided after more detailed information is requested. Customer provides information that seems minimal, possibly false or inconsistent.
15.	Customer acting on behalf of a third party	Customer has vague knowledge about amount of money involved in the transaction. Customer taking instructions for conducting transactions, Customer is accompanied by unrelated individuals
16.	Multiple customers working as a group	Multiple customers arrive together but pretend to ignore each other
17.	Customer avoiding nearer Branches	Customer travels unexplained distances to conduct transactions.
18.	Customer offers different identifications on different occasions	Customer offers different identifications on different occasions in an apparent attempt to avoid linkage of multiple transactions.
19.	Customer wants to avoid reporting	Customer makes inquiries or tries to convince staff to avoid reporting.
20.	Customer could not explain source of funds	Customer could not explain source of funds
21	Transaction is unnecessarily complex	Transaction is unnecessarily Complex for its stated purpose
22.	Transaction has no economic rationale	The amounts or frequency or the stated reason of the transaction does not make sense for the particular customer
23.	Transaction inconsistent with business	Transaction involving movement of which is inconsistent with the customer's business
24.	Unapproved inward remittance in NPO	Foreign remittance received by NPO not approved by FCRA

25.	Complaint received from public	Complaint received from public for abuse of account for committing fraud etc.
26	Alert raised by agent	Alert raised by agent for suspicion
27.	Alert raised by other institution	Alert raised by other institutions, subsidiaries or business associates including cross border referral

Branches should report any of the above suspicious behavior of the customer/ walk-in-customer noticed by them through CBS menu "AMLALERT".

➢ **Format for filing of STRs in electronic format:**

Bank will use Electronic Format as prepared by FIU-IND, New Delhi

➢ **Manner and Procedure of filing STRs:**

a. AML Team at Head Office will prepare STRs in **Electronic** Format and forward it to the Principal Officer i.e. not more than 7 days from the date of arrival of conclusion that the transaction is suspicious one.

b. Principal Officer will examine such STRs and will record his reasons for treating transaction or a series of transactions as suspicious and will report to FIU-IND, New Delhi within 7 days of arriving at conclusion that **any transaction, whether cash or non- cash, or a series of transactions integrally connected are** suspicious one. **It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report generated.**

c. Bank would not put any restrictions on operations in the accounts where an STR has been filed. Bank and its employees would keep the fact of furnishing of STR strictly confidential, as required under PML Rules. It should be ensured that there is no tipping off to the customer at any level.

➢ **Generation of Alerts through System for detection of Suspicious Transactions**:

a. As a part of transaction monitoring mechanism, bank has put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customer

b. Bank has procured web based AML software FCDMS (Financial Crime Detection and Management System)for CBS for generating / throwing alerts on the Risk Views defined by the bank for effective identification and reporting of suspicious transactions.

c. Alerts generated by the AMLOCK SYSTEM will be assigned to L1 user for scrutiny/process the generated alert, AML CELL examine and report STR cases to Principal Officer for finalized case as STR and then reporting of STRs to FIU-IND, New Delhi.

➢ **Time Schedule for Filing Suspicious Transaction Reports (STR)**

Bank will adhere to the following time schedule and procedure for reporting STRs to FIU-IND:

a. The Suspicious Transaction Report (STR) will be furnished within -7- days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal officer will record his reasons for treating any transaction or a series of transactions as suspicious. It will be ensured that there

is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from the **AML CELL.**
b. AML CELL will submit the STRs to the Principal Officer after validation in seven days **of arriving at a conclusion that any transaction is suspicious one**.

22.3. Counterfeit Currency Reports (CCRs)

All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine will be reported by the Principal Officer (PO) to FIU-IND in the specified format (Counterfeit Currency Report – CCR) by 15th of the succeeding month. These cash transactions will also include transactions where forgery of valuable security or documents has taken place and will be reported in the form as prescribed by bank to FIU-IND for the present. In this regards, our Bank has issued Circular no. HO:OPR-10/06/143 Dtd. 16.07.2018.

In no case, the counterfeit notes will be returned to the tenderer or destroyed by the branches/ currency chests. An acknowledgement receipt must be issued to the tenderer, after stamping the note. The receipt, in running serials numbers, should be authenticated by the cashier and the tenderer. The receipt is to be issued even in cases where the tenderer is unwilling to countersign it.

➢ **Manner and Procedure of filing CCRs:**

Branches will submit Detection of Counterfeit Currency at the end of the month to their respective District Nodal Officer who, in turn, is further required to send the reports to their respective Regional Offices. Regional Offices in turn, will consolidate the CCRs and forward it to FNVC Cell at Head Office, Ajmer. Bank's Compliance Manager/Principal Officer to report the CCRs to FIU-IND by the 15th of the succeeding month.

22.4.Non-Profit Organization Transaction Report (NTR)

The report of all transactions involving receipt by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency is being submitted every month to the Director, FIU-IND by 15th of the succeeding month in the prescribed format.

22.5 Cross-border Wire Transfer Report (EFT)

Cross-border Wire Transfer Report is required to be filed with FIU-IND by 15th of succeeding month for all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India. The Principal Officer at Head Office submits EFT to the Director FIU-IND, New Delhi.

23. Miscellaneous

Secrecy Obligations and Sharing of Information:

(a) Branches are advised to maintain secrecy regarding the customer information which arises out of the contractual relationship between the Banker and customer.

(b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling or for any other purpose without express permission of the customer.

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

(d) The exceptions to the said rule advised by RBI are as under:

- Where disclosure is under compulsion of law.
- Where there is a duty to the public to disclose,
- The interest of bank requires disclosure and
- Where the disclosure is made with the express or implied consent of the customer.

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

Bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. 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.

Our Bank is registered with Central KYC Records Registry(CKYCR) and Financial Institute (FI) Code "**IN0869**" allotted by CKYCR.

Bank has established CKYC Cell for reporting (uploading of customer data on CKYC portal), monitoring and compliance of the instructions/guidelines issued by Central KYC Records Registry from time to time.

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

Earlier in 2010, the United States of America (USA) enacted a law known as Foreign Account Tax Compliance Act (referred as FATCA) with the objective of tackling tax evasion through obtaining information in respect offshore financial accounts maintained by residents and citizens of USA.

Similarly, India also signed a multilateral agreement on 3rd June 2015 to exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters under **Common Reporting Standard (CRS).**

Necessary amendments have been made in Income Tax Rules 1962 by CBDT (Central Board of Direct Taxes) for its smooth & mandatory implementation in India by Financial Institutions. Our bank also comply with guidelines on FATCA & CRS inter alia with reporting requirements as provided in Rules 114F to 114H and Form 61B of Income Tax Rules, 1962.

FATCA-CRS Declaration to be obtained from the Individuals (including sole proprietor) & Entities along with all the beneficial owner/s separately before opening a new customer ID/account. The form should be duly filled in & signed by the applicant with evidence wherever required. In case of joint account holders, declaration must be obtained separately from all of them.

FATCA-CRS Due Diligence in pre-existing accounts:

The accounts opened before 01.07.2014 are considered as pre-existing accounts under FATCA & accounts opened before 01.01.2016 are considered pre-existing under CRS. For pre-existing accounts, bank is allowed to rely on the information available on the Banks' record.

Branches need to identify the Reportable Accounts by carrying out check based on the -7- indicia search in their electronic data base. The -7- indicia are

(A) FATCA

1. Identification of the Account Holder as U.S. citizen or resident
2. Unambiguous indication of a U.S. place of birth
3. Current U.S. mailing or residence address (including a U.S. post office box)
4. Current U.S. telephone number
5. Standing instructions to transfer funds to an account maintained in the United States.
6. Current effective power of attorney or signatory authority granted to a person with a U.S. address
7. An "in-care-of" of "hold mail" address (of U.S.) that is the sole address the Bank has on file for the Account Holder.

(B) CRS

1. Identification of the Account Holder as Tax Resident in any other jurisdiction outside india/U.S.
2. Unambiguous indication of a place of birth in any jurisdiction outside India/U.S.
3. Current mailing or residence address in any jurisdiction outside India/U.S.(including a post office box)
4. Current telephone number in a jurisdiction outside India/U.S.
5. Standing instructions to transfer funds to an account maintained in any other jurisdiction outside India/United States.
6. Current effective power of attorney or signatory authority granted to a person with address in any other jurisdiction outside India/U.S.
7. An "in-care-of" of "hold mail" address in any jurisdiction outside India/U.S.& that is the sole address the bank has on file for the Account Holder.

In pre-existing accounts, where anyone or more of such indicia are found, due diligence is to be carried out & **to identify the reportable accounts, a declaration to be obtained from the customer for his/her tax resident status. Same declaration form will be used for this purpose as being taken with the new account opening form.**

Whenever, change in circumstance occurs in situation of account holder (i.e. change in his/her/their tax residency), a fresh FATCA-CRS declaration to be obtained. **Enrichment of FATCA-CRS declaration through HFATCA menu option and keeping the physical record is mandatory**

➢ **Freezing/blocking of accounts: FATCA non-compliance** -branches to ensure that all individual & entity accounts opened on or after 01-07-2014 but before the date of entry into force of FATCA agreement i.e. 31-08-2015, self-certification has been obtained. Where it is not provided by the account holder, account must be blocked w.e.f. 01st May 2017. (Blocking of account would mean that no customer initiated transaction would be allowed after 30th April 2017 unless self-certification is submitted by the account holder)

25. Selling Third party products:

Bank 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:
(a) the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand
(b) transaction details of sale of third party products and related records shall be maintained as prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:
(i) The nature of transactions;
(ii) The amount of transaction and the currency in which it was denominated;
(iii) The date on which the transaction was conducted; and
(iv) The parties to the transaction.
(c) AML software capable of capturing, generating and analyzing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.
(d) transactions involving rupees fifty thousand and above shall be undertaken only by:
- debit to customers' account or against cheques; and
- obtaining and verifying the PAN given by the account-based as well as walk-in customers.

(e) Instruction at 'd' above shall also apply to sale of Banks' 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.

Branches are advised to take careful note of the above directive of Reserve Bank of India for strict and meticulous compliance.

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

a.) The 'at par' facility offered by commercial banks to co-operative banks is in the nature of correspondent banking arrangements, bank will have to monitor and review such arrangements to assess the risks including credit risk and reputational risk arising therefrom.

b.) For this purpose, bank will retain the right to verify the records maintained by the client cooperative banks/ societies for compliance with the extant instructions on KYC and AML under such arrangements.

c.) Cooperative Banks shall 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 customer's accounts,**
- **for walk-in customers against cash for less than rupees fifty thousand per individual.**

d.) Cooperative Banks shall 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 honoring such instruments.**

e.) Ensure that 'at par' cheques issued are crossed 'account payee' irrespective of the amount involved.

The branches/offices are advised to ensure the above guidelines while extending such services to **co-operative banks and** obtain undertaking or incorporate the same in MOU to be undertaken with them for its compliance.

27. Operation of bank accounts and "Money Mules"

a. "Money Mules" 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 to act as "money mules". In some cases these third parties may be innocent while in others they may be having complicity with the criminals.

b. In a money mule transaction, an individual with a bank account is recruited to use cheque deposits or wire transfers and then transfer these funds to accounts held on behalf of another person or to other individuals, minus a certain commission payment. Money mules by such persons are recruited by a variety of methods viz. spam e-mails, advertisements on genuine recruitment websites, social networking sites, instant messaging and advertisement in newspapers. When caught, these money mules often have their bank accounts suspended, causing inconvenience and potential financial loss, apart from facing legal action for being part of a fraud. Many a times the address and contact details of such mules are found to be fake or not up to date, making it difficult for investigating agencies to locate the account holder.

c. To minimize operations of such Money Mules, bank is to strictly adhere to the KYC-AML-CFT guidelines issued from time to time and to those relating to periodical updation of customer identification data after the account is opened and also for monitoring of transactions to protect the bank and customers from misuse by such fraudsters.

28. Walk-in Customers

'Walk-in Customer' means a person who does not have an account-based relation with the Bank but undertakes transaction with the Bank.

In case of a Non account based customer i.e. walk-in customer approaching for such single/ one-off transaction, where amount of transaction is equal to or exceeds Rs 50,000/- whether conducted as single transaction or several transactions appear to be connected, the customer identity and address should be obtained and verified.

However, if the branch has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs 50,000/- the branch will verify the identity and address of the customer and also consider filing a suspicious transaction report (STR) to FIU-IND through Principal Officer.

Bank no longer knows the true identity: In the circumstances when the Bank believes that it would no longer be satisfied that it knows the true identity of the account holder, the bank will also file an STR with FIU-IND.

29. Other Instructions:

29.1 Correspondent Banking and Shell Bank

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:

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

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

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

(d) 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.

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

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

(g) It shall be ensured that the correspondent banks do not permit their accounts to be used by **shell banks (i.e. a bank which is incorporated in a country where it has no physical presence and is not affiliated to any regulated financial group).**

(h) 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.

(i) 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.

29.2. Issue of Demand Drafts / Bankers Cheques etc. for Rs.50,000/- or more

(a) Branches should ensure that remittance of funds by way of demand draft, Banker's cheque, mail/ telegraphic transfer/(Electronic Transfer)/ NEFT/ IMPS or any other mode and issue of travelers' cheques for value of Rs.50,000/- and above is effected by debit to the customer's account or against cheques and not against cash payments.

(b) 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.

(c) transactions involving rupees fifty thousand and above shall be undertaken only by obtaining and verifying the PAN given by the account based as well as walk-in customers.

Instruction at **'c'** above shall also apply to sale of Bank's own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for Rupees Fifty Thousand and above.

Branches are advised to take careful note of the above directive of Reserve Bank of India for strict and meticulous compliance.

Branches should not make payment of cheques/ demand drafts/ banker's cheques, if they are presented beyond the period of three months from the date of such instrument.

29.3 Wire Transfer

Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. The originator and the beneficiary may be the same person.

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

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

(ii) Cross - border transfer means any wire transfer where the originator and the beneficiary bank or financial institution is located in different countries. It may include any chain of wire transfers that has at least one cross-border element.

Bank shall ensure following while effecting wire transfer:

(a) 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.

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

(c) 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.

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

(e) 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.

(f) 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.

(g) 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.

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

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

(j) 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.

Branches are advised for strict and meticulous compliance of the above directions of RBI.

30. General Guidelines

1. Bank will ensure that the information collected from the customer for the purpose of opening of account is treated as confidential and details thereof will not to be divulged for cross selling or any other like purposes.

2. Bank will further ensure that information sought from the customer is relevant to the perceived risk and not intrusive but in conformity with the guidelines issued in this regard.

3. Any other information from the customer will be sought by bank separately with his/her consent and after opening the account.

4. Bank will ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer/NEFT/IMPS(**electronic fund transfer**) or any other mode for value of Rs. 50,000/- (Rupees fifty thousand) and above is 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.

5. Bank will ensure that **Permanent Account Number (PAN)** is invariably quoted by the customer while:

a. Opening of an Account (other than a Time Deposit Account) with the bank.

b. Opening Time Deposit Account exceeding Rs. 50000/- or aggregating to more than Rs. 5,00,000/- during a financial year with the Bank.

c. Depositing cash amount exceeding Rs. 50000/- during any one day for purchase of Bank Drafts or Banker's Cheques from the bank.

d. Depositing cash in an account exceeding Rs. 50000/- in any one day.

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.

In case, customer is not having PAN or equivalent e-document in his/her name, then Bank will obtain declaration in Form No.60 from the customer for each such transaction.

Bank will verify PAN quoted by the customer, with the original PAN Card / PAN Allotment Letter and retain copy thereof for having ensured due diligence in this regard. Further, verification of PAN through the menu "PANVAL" is must.

Bank will invariably capture PAN in Computer system at appropriate field **and verify the same through NSDL Server while opening of accounts/ updating the PAN details,** as well as periodically updating KYC in the account.

6. 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.

7. Collection of Account Payee Cheques

Account payee cheques for any person other than the payee constituents will not be collected by the branches.

8.Avoiding hardship to customers:

While complying with the KYC-AML-CFT guidelines, branches should keep in mind the spirit of the instructions issued by the Reserve Bank of India so as to avoid undue hardships to individuals who are otherwise classified as Low Risk customers.

9.Sensitizing customers:

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

10.Employee training:

Bank has on going employee training programme so that the members of staff are adequately trained in AML/CFT policy. Head Office periodically conducts training programmes for the Regional AML teams in matters relating to reporting requirements and scrutiny of AML alerts from STR angle. The executives from Head Office also visit the training establishments to share KYC-AML-CFT challenges before the Bank.

11. Hiring of Employees

As RBI has prescribed KYC Norms / AML Standards / CFT Measures with sole objective to ensure that criminals are not allowed to misuse the banking channels, bank will also ensure that adequate screening mechanism is put in place as an integral part of its recruitment / hiring process of personnel to obviate probability of recruiting such criminals in the bank.

At the time of joining/Recruitment the applicant is required to fill up the service entry forms wherein he /she is required to declare specifically for the question:

"Have you ever been arrested or kept under detention / was imprisoned or bound down/fined/convicted by a Court of Law for any offence or FIR lodged/compliant registered/ charges framed against you or any criminal case pending against you before any Court of Law/authority or debarred/disqualified by the Public Service Commission from appearing at its examination selection or debarred from taking any examination or restricted by any authority / any institution/ terminated from service by any previous employer for any criminal offence/ indiscipline or any other acts of misconduct etc....."

Apart from the above, the Bank has a set procedure for verification of the antecedent of the candidate from the Police authorities for confirmation of the employee in Bank service.

Bank also ask to provide two reference certificates known to the bank and the payment of the salary is credited online in the account of employee directly through Payroll. System will do the screening against watch list while opening of account.

12.Provisions of FCRA

Branches should ensure that the provisions of the Foreign Contribution (Regulation) Act, 2010 and FCRR-2011 wherever applicable, are strictly adhered to.

31. Review of Policy:

The policy will be effective for two year from the date of approval by the Board. Policy will be reviewed by Board periodically. Chairman will be vested with the authority to effect any subsequent modification in this Policy Document till the policy is revised again by the Board.

Any circular/ guidelines issued on KYC-AML-CFT and Obligation of Bank under PMLA, 2002 by Reserve Bank of India/ Government of India will automatically be a part of this policy with immediate effect.

Bank will issue guidelines from time to time on KYC-AML-CFT standards and measures in line with guidelines received from Regulator for the purpose of its compliance by its branches/offices.

Further, project of implementation of AML Solution has been implemented in our Bank. Chairman will be vested with the authority to effect changes in the reporting structure or to decide about procuring / developing another / additional software applications and will be assisted by committee of following executives.

1. General Manager (Principal Officer)
2. General Manager
3. Vigilance Chief Manager (Central Internal Audit Division)
4. Chief Manager (IT & CBS)
5. Chief Manager (Operation).

२७.

ANNEXURE A

Digital KYC Process (To be discussed-Digital KYC is not started in our bank)

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

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

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

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

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

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

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

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

I. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' 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 RE shall not be used for customer signature. The RE must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

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

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

L. The authorized officer of the Bank shall check and verify that : - (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.;

M. On Successful verification, the CAF 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.

Annexure - B
KYC documents for eligible FPIs under PIS

		FPI Type		
Document Type		**Category I**	**Category II**	**Category III**
Entity Level	Constitutive Documents (Memorandum and Articles of Association, Certificate of Incorporation etc.)	Mandatory	Mandatory	Mandatory
	Proof of Address	Mandatory (Power of Attorney {PoA} mentioning the address is acceptable as address proof)	Mandatory (Power of Attorney mentioning the address is acceptable as address proof)	Mandatory other than Power of Attorney
	PAN	Mandatory	Mandatory	Mandatory
	Financial Data	Exempted *	Exempted *	Mandatory
	SEBI Registration Certificate	Mandatory	Mandatory	Mandatory
	Board Resolution @@	Exempted *	Mandatory	Mandatory
Senior Management (Whole Time Directors/ Partners/ Trustees/ etc.)	List	Mandatory	Mandatory	Mandatory
	Proof of Identity	Exempted *	Exempted *	Entity declares* on letter head full name, nationality, date of birth or submits photo identity proof
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *
Authorized Signatories	List and Signatures	Mandatory - list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory - list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory
	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *

Ultimate Beneficial Owner (UBO)	List	Exempted *	Mandatory (can declare "no UBO over 25%")	Mandatory
	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *

* Not required while opening the bank account. However, FPIs concerned may submit an undertaking that upon demand by Regulators/Law Enforcement Agencies the relative document/s would be submitted to the bank.
@@ FPIs from certain jurisdictions where the practice of passing Board Resolution for the purpose of opening bank accounts etc. is not in vogue, may submit 'Power of Attorney granted to Global Custodian/Local Custodian in lieu of Board Resolution'

Category	**Eligible Foreign Investors**
I.	Government and Government related foreign investors such as Foreign Central Banks, Governmental Agencies, Sovereign Wealth Funds, International/ Multilateral Organizations/ Agencies.
II.	a) Appropriately regulated broad based funds such as Mutual Funds, Investment Trusts, Insurance /Reinsurance Companies, Other Broad Based Funds etc. b) Appropriately regulated entities such as Banks, Asset Management Companies, Investment Managers/ Advisors, Portfolio Managers etc. c) Broad based funds whose investment manager is appropriately regulated. d) University Funds and Pension Funds. e) University related Endowments already registered with SEBI as FII/Sub Account.
III.	All other eligible foreign investors investing in India under PIS route not eligible under Category I and II such as Endowments, Charitable Societies/Trust, Foundations, Corporate Bodies, Trusts, Individuals, Family Offices, etc.

Annex C
File No. 14014/01/2019/CFT
Government of India
Ministry of Home Affairs
CTCR Division

North Block, New Delhi.
Dated: the 2nd February, 2021

ORDER

Subject: - Procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 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 —

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

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.

2. In order to ensure expeditious and effective implementation of the provisions of Section 51A, a revised procedure is outlined below in supersession of earlier orders and guidelines on the subject:

3. **Appointment and communication details of the UAPA Nodal Officers**:

3.1 The Joint Secretary (CTCR), Ministry of Home Affairs would be the Central [designated] Nodal Officer for the UAPA **[Telephone Number: 011-23092548, 011-23092551 (Fax), email address: jsctcr-mha@gov.in].**

3.2 The Ministry of External Affairs, Department of Economic Affairs, Ministry of Corporate Affairs, Foreigners Division of MHA, FIU-IND, Central Board of Indirect Taxes and Customs (CBIC) and Financial Regulators (RBI, SEBI and IRDA) shall appoint a UAPA Nodal Officer and communicate the name and contact details to the Central [designated] Nodal Officer for the UAPA.

3.4 All the States and UTs shall 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 Central [designated] Nodal Officer for the UAPA.

3.5 The Central [designated] Nodal Officer for the UAPA shall maintain the consolidated list of all UAPA Nodal Officers and forward the list to all other UAPA Nodal Officers, in July every year or as and when the list is updated and shall cause the amended list of UAPA Nodal Officers circulated to all the Nodal Officers.

3.6 The Financial Regulators shall forward the consolidated list of UAPA Nodal Officers to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies.

3.7 The Regulators of the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs shall forward the consolidated list of UAPA Nodal Officers to the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs.

4. **Communication of the list of designated individuals/entities**:

4.1 The Ministry of External Affairs shall update the list of individuals and entities subject to the UN sanction measures whenever changes are made in the lists by the UNSC 1267 Committee pertaining to Al Qaida and Da'esh and the UNSC 1988 Committee pertaining to Taliban. On such revisions, the Ministry of External Affairs would electronically forward the changes without delay to the designated Nodal Officers in the Ministry of Corporate Affairs, CBIC, Financial Regulators, FIU–IND, CTCR Division and Foreigners Division in MHA.

4.2 The Financial Regulators shall forward the list of designated persons as mentioned in Para 4(i) above, without delay to the banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies.

4.3 The Central [designated] Nodal Officer for the UAPA shall forward the designated list as mentioned in Para 4(i) above, to all the UAPA Nodal Officers of States/UTs without delay.

4.4 The UAPA Nodal Officer in Foreigners Division of MHA shall forward the designated list as mentioned in Para 4(i) above, to the immigration authorities and security agencies without delay.

4.5 The Regulators of the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs shall forward the list of designated persons as mentioned in Para 4(i) above, to the real estate agents, dealers in precious metals & stones (DPMS) and DNFBPs without delay.

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

5.1 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.

5.2 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.

5.3 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.

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

6.1 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.

6.2 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.

6.3 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.

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

6.5 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.

6.6 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.

7. **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 6.2 to 6.5 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 6.2 to 6.5 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 6.2 to 6.5 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 paragraph 6.2 to 6.5 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 paragraph 6.2 to 6.5 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 paragraph 6.2 to 6.5 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 paragraph 6.2 to 6.5 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 paragraph 8 to 10 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 paragraph 6.2 to 6.5 above.

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

8.1 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.

8.2 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.

8.3 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.

9. 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 5 and 6 above shall be followed.

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

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

10.1 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:-

(a) 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;

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

10.2. 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;

11. **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:**

11.1 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.

11.2 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.

11.3 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.

12. **Regarding prevention of entry into or transit through India:**

12.1 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.

12.2 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.

211.

13. **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.

14. **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.

15. All concerned are requested to ensure strict compliance of this order.

(Ashutosh Agnihotri)
Joint Secretary to the Government of India

Annexure – D

List of "Officially Valid Documents" to be obtained for Account Opening

It must be noted that only documents mentioned this list should be accepted by the branches while opening any new account and periodical updation of identification data of existing Account Holders / Customer

Branches would not have the discretion to accept any other document for this purpose.

Mandatory Documents for Individuals other than exempted category	□ Aadhaar/ Aadhaar Enrolment Number □ Permanent Account Number (PAN) / FORM 60 Note: Aadhaar/ Aadhaar Enrolment Number is exempted for the residents in the state of Jammu and Kashmir/ Assam/ Meghalaya. They will be required to submit any of the OVDs, mentioned below, for opening of the accounts. Note 2: Aadhaar number will not be sought from individuals who are not 'residents' as defined under Aadhaar Act. A declaration to the effect will be obtained by the Bank.	
In case of Foreign Students	□ An Identity Card issued by college / institution. □ An admission letter for the course mentioning duration of course for which he/ she is admitted by the Institute / College. □ Copy of Passport and copy of Visa. □ An allotment letter on letter head of the institution/ college for allotment of hostel accommodation duly singed by the authorized signatory, mentioning detailed address and location of hostel, room no. etc. and date of allotment of hostel accommodation etc. or a valid address proof giving local address in form of rent agreement within 30 days of opening of the account.	
For NRI / Foreign Tourist **FOR PIO/OCI**	□ Passport □ Valid Visa □ PAN/FORM 60 □ Passport □ PIO CARD/OCI CARD □ PAN/FORM 60	**Address proof mentioning the current overseas address (any one of the below)** □ Documents issued by Govt. Deptt. of foreign jurisdictions i.e. Driving License, National Identification Card, Social Security Card, Employee Card and Labour Card, Tax Residency Certificate etc. having Name and Address of the Applicant □ Letter issued by Foreign Embassies or Mission in India having Name and Address of the Applicant □ Utility bill of any service provider i.e. electricity, telephone, postpaid mobile phone, piped gas, water bill (not more than two months old) □ Property/ Municipal Tax Receipt □ Letter of allotment of accommodation/ Leave and License agreements allotting official accommodation from employer

		issued by State or Central Govt. departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies
For Foreign Nationals	Aadhaar/ Aadhaar Enrollment Number (If customer is not eligible of Aadhaar at the time of opening of the account, a declaration cum undertaking is to be obtained as per format provided.) ☐ PAN/FORM 60 ☐ Valid Foreign Passport ☐ Valid Indian Visa	**Address proof mentioning the current overseas address (any one)** ☐ Foreign Driving License ☐ Documents issued by Govt. Deptt. of foreign jurisdictions i.e. National Identification Card, Green Card and Social Security Card etc. having Name and Address of the Applicant ☐ Letter Issued by Foreign Embassies or Mission in India having Name and Address of the Applicant
	(If Aadhaar/ Aadhaar Enrolment Number is not provided, FRRO/ FRO Certificate/Permit/ Indian Driving License/ any Deemed OVD mentioned below, is required to be provided for Indian Address Proof.)	
Accounts of Companies	**(All following documents to be obtained)** ☐ Certificate of Incorporation ☐ Memorandum & Articles of Association. ☐ PAN No. of the Firm ☐ Resolution of the Board of Directors and Power of Attorney granted to its managers, officers or employees to transact on its behalf; and ☐ Aadhaar Number/ Aadhaar Enrolment Number and PAN*/ FORM 60 of the managers, officers or employees holding an attorney to transact on its behalf with his / her photograph	
Accounts of Sole Proprietary firms	**(Any two of the following documents to be obtained)** ☐ Proof of the name, address and activity of the concern, like registration certificate (in case of registered concern), ☐ Certificate of / license issued by the municipal authorities under Shop & Establishment Act, ☐ Sales and income tax returns, ☐ CST / VAT certificate, ☐ Certificate / registration document issued by Sales Tax / Service Tax /Professional Tax authorities. ☐ License issued by the Registering authority like certificate of Practice issued by Indian Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, etc. Registration / licensing document issued in the name of proprietary concern by the Central Government or State Government Authority / Department, IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an Identity document. ☐ The complete Income Tax return (not just the acknowledgement)	

	in the name of Sole Proprietor where the Firm's income is reflected, duly Authenticated/Acknowledged by the Income Tax Authorities. □ Utility bills such as electricity, water, and landline telephone bills (Not more than two months old) in the name of the proprietary concern. **OR** In case 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 would have to undertake contact point verification, collect information to establish the existence of such firm, confirm, clarify and satisfy that the business activity has been verified from the address of the proprietary concern. **AND** Aadhaar Number/ Aadhaar Enrolment Number and PAN/ FORM 60 of the proprietor.
Accounts of Partnership firms(Registered)	**(All following documents to be obtained)** □ Registration certificate, □ Partnership deed; and □ PAN No. of the Firm, □ Aadhaar Number/ Aadhaar Enrolment Number and PAN*/ FORM60 of the person holding an Attorney to transact on its behalf with his/ her photograph)
Accounts of Trusts & Foundations.	**(All following documents to be obtained)** □ Registration Certificate □ Trust Deed; □ PAN No. of Entity □ Aadhaar Number/ Aadhaar Enrollment Number and PAN*/ FORM60 of the Trustees, settlers, beneficiaries and persons holding Power of Attorney, Founders/Managers, Directors/Signatories with his/her photograph
Accounts of Unincorporated Associations or body of individuals/Society / Clubs. ***For unregistered entities (whether partnership firm, trusts, foundations etc.)**	**(All following documents to be obtained)** □ Resolution of the Managing body of such association or body of individuals; □ PAN □ Power of Attorney granted to transact on its behalf; □ Aadhaar Number/ Aadhaar Enrolment Number and PAN*/ FORM 60 of the Office bearers / Signatories and persons holding Power of Attorney, if any with his/her photograph in respect of the person holding an Attorney to transact on its behalf; □ Any one of the below mentioned list of documents to collectively establish the legal existence of such an associations or body of individuals. □ Partnership Deed/ Trust Deed □ Certificate of / license issued by the municipal authorities under Shop & Establishment Act, □ Sales Tax Returns, □ CST / VAT certificates □ Certificate / registration document issued by Sales Tax / Service

	Tax /Professional Tax authorities. □ License issued by the Registering authority like certificate of Practice issued by Indian Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, etc. □ The complete Income Tax return (not just the acknowledgement) in the name of Sole Proprietor where the Firm's income is reflected, duly Authenticated/ Acknowledged by the Income Tax Authorities.
Accounts of Hindu Undivided Family	**(All following documents to be obtained)** □ PAN Card in the name of HUF. □ Declaration from the Karta. □ Aadhaar Number/ Aadhaar Enrollment Number and PAN*/ FORM 60 of the Karta with his / her photograph □ HUF Letter/ Declaration signed by all the coparcener and Karta
Accounts of the Government or its Departments, societies, universities and local bodies like village panchayats etc.	a. Document showing name of the person authorized to act on behalf of the Government or its Departments, societies, universities and local bodies like village panchayats; b. Aadhaar/ PAN/ Officially valid documents for proof of identity and address in respect of the person holding an attorney to transact on its behalf and **c.** Any document to establish the legal existence of such an entity/ juridical person.
Officially Valid Documents (OVDs) (Any one)	□Passport □ Driving license with photo □ Voter's Identity Card issued by Election Commission of India, □ Job card issued by NREGA duly signed by an officer of the State Government. □ Letter issued by the National Population Register containing details of Name and Address. Proof of possession of Aadhaar number may submit in such form as are issued by the Unique Identification Authority of India.
Deemed Officially Valid Documents, In case OVD does not contains updated /current address. (At least one document.)	□Utility bill of any service provider i.e. electricity, telephone, postpaid mobile phone, piped gas, water bill (not more than two months old)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 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; the customer shall submit OVD with current address within a period of three months of submitting the documents specified above.

Annexure – F
List of High / Medium / Low Risk Countries.

	High Risk Countries		High Risk Countries		High Risk Countries
1	Afghanistan	16	Israel	31	Somalia.
2	Andorra	17	Kyrgyzstan	32	St. Christopher & Nevis.
3	Chad.	18	Lebanon	33	St. Lucia.
4	Central African Republic.	19	Liberia.	34	Sudan
5	Congo Republic	20	Libya	35	Syria
6	Cote De Ivoire.	21	Malawi	36	Timor Leste
7	Democratic Republic of Congo	22	Marshall Islands	37	Turkmenistan
8	Eritrea.	23	Micronesia	38	Ukraine
9	Georgia	24	Moldova	39	Venezuela
10	Greece	25	Montenegro	40	Yemen
11	Grenada	26	Nauru	41	Zimbabwe
12	Guinea Bissau.	27	North Korea.	42	Anguilla
13	Guinea.	28	Palestine	43	Turks and Caicos (UK)
14	Iran	29	Pakistan		
15	Iraq	30	Serbia		

	Medium Risk Countries		Medium Risk Countries		Medium Risk Countries
1	Albania	30	Gambia	59	Portugal
2	Algeria	31	Ghana.	60	Reunion Islands
3	Angola	32	Guatemala.	61	Romania.
4	Antigua and Barbuda.	33	Guyana	62	Rwanda.
5	Argentina	34	Haiti.	63	Samoa.
6	Armenia	35	Honduras.	64	SaoTome& Principe.
7	Azerbaijan.	36	Iceland	65	Senegal.
8	Barbados	37	Jamaica.	66	Seychelles.
9	Belarus	38	Jordan.	67	Sierra Leone.
10	Belize	39	Kazakhstan	68	Slovenia
11	Benin	40	Kenya.	69	Solomon Islands.
12	Bolivia.	41	Laos	70	St. Vincent & Grenadine
13	Bosnia & Herzegovina.	42	Latvia	71	Suriname.
14	Burkina Faso.	43	Lesotho	72	Swaziland.
15	Burundi.	44	Macedonia.	73	Tajikistan.
16	Cambodia.	45	Madagascar.	74	Tanzania.
17	Cameroon	46	Maldives	75	Togo.
18	Cape Verde.	47	Mali.	76	Tunisia
19	Comoros.	48	Malta	77	Turkey
20	Cuba.	49	Mauritania.	78	Uganda.
21	Cyprus	50	Monaco	79	Uzbekistan.
22	Djibouti.	51	Mongolia.	80	Vanuatu.
23	Dominica.	52	Mozambique.	81	Zambia
24	Ecuador.	53	Myanmar.	82	Cook Islands (NZ)
25	Egypt.	54	Namibia.	83	Fiji.
26	El Salvador.	55	Nepal	84	Gabon.

27	Equatorial Guinea.	56	Nicaragua	85	Papua New Guinea.
28	Estonia.	57	Niger.	86	Paraguay.
29	Ethiopia.	58	Nigeria.		

	Low Risk Countries		**Low Risk Countries**		**Low Risk Countries**
1	Aruba	35	Gibraltar (UK)	69	Russia
2	Australia.	36	Guadeloupe (France)	70	San Marino (Italy)
3	Austria.	37	Guam.	71	Saudi Arabia.
4	Bahamas	38	Hong Kong.	72	Singapore.
5	Bahrain	39	Hungary.	73	Slovenia.
6	Bangladesh	40	India.	74	South Africa.
7	Belgium.	41	Indonesia	75	South Korea.
8	Bermuda.	42	Ireland	76	Spain.
9	Bhutan.	43	Italy	77	Sri Lanka.
10	Botswana	44	Japan	78	Sweden.
11	Brazil	45	Kiribati	79	Switzerland.
12	British Pacific Islands.	46	Kuwait	80	Taiwan.
13	British Virgin Islands	47	Liechtenstein	81	Thailand
14	Brunei.	48	Lithuania	82	Tonga
15	Bulgaria	49	Luxembourg	83	Trinidad &Tobago.
16	Canada.	50	Macao.	84	United Arab Emirates
17	Canary Islands.	51	Malaysia	85	United Kingdom
18	Cayman Islands (UK)	52	Martinique (France)	86	United States of America
19	Channel Isles (UK)	53	Mauritius.	87	Uruguay
20	Chile.	54	Mayotte.	88	U.S. Pacific Islands.
21	China.	55	Mexico.	89	U.S. Virgin Islands.
22	Christmas Islands (Australia)	56	Morocco.	90	Vatican City.
23	Cocos/ Keeling Island (Australia)	57	Netherland Antilles.	91	Vietnam
24	Colombia	58	Netherlands.	92	American Samoa
25	Costa Rica	59	New Zealand.	93	Faroe Islands.
26	Croatia	60	Norfolk Islands.	94	French Guiana
27	Czech Republic.	61	Norway	95	French South Atlantic Territories
28	Denmark	62	Oman.	96	Greenland
29	Dominican Republic	63	Panama	97	Heard Island and McDonald Island (Australia)

30	Falkland Islands	64	Peru	98	Montserrat.
31	Finland	65	Philippines.	99	St. Helena & Ascension.
32	France	66	Poland.	100	St. Pierre & Mizuelon.
33	French Polynesia (France)	67	Puerto Rico.		
34	Germany	68	Qatar.		

ANNEXURE – F-1

RISK CATEGORISATION OF CUSTOMERS BASED ON ANNUAL INCOME OR TURN OVER IN THE ACCOUNT OF CUSTOMER

HIGH RISK CUSTOMERS

Category / Constitution	Annual Income / Turn Over
Individuals	Rs.100/- Lakhs & above.
Sole Proprietary concerns	Rs. 5/- Crores & above.
Partnership firms	Rs.10/- Crores & above.
Limited Companies (both public & private)	Rs. 50/- Crores & above.
Trusts	Irrespective of Turnover
Associations, Clubs etc.	Irrespective of Turnover.

MEDIUM RISK CUSTOMERS

Category / Constitution	Annual Income / Turn Over
Individuals	Above Rs. 10/- Lakhs but below Rs. 100/- lakhs.
Sole Proprietary concerns	Above Rs. 1/- Crore but below Rs. 5/- Crores.
Partnership firms	Above Rs. 5/- Crores but below Rs. 10/- Crores.
Limited Companies (both public & private)	Above Rs. 10/- Crores but below Rs. 50/- Crores.

LOW RISK CUSTOMERS

Category / Constitution	Annual Income / Turn Over
Individuals	Upto and inclusive of Rs. 10/- Lakhs.
Sole Proprietary concerns	Upto and inclusive of Rs. 1/- Crore.
Partnership firms	Upto and inclusive of Rs. 5/- Crores.
Limited Companies (both public & private)	Upto and inclusive of Rs. 10/- Crores.

ANNEXURE – F-2

Indicative List of High / Medium risk customers:

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

Characteristics of High Risk Customers

1. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc.
2. Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of and for coping with terrorist activities
3. Individuals and entities in watch lists issued by Interpol and other similar international organizations
4. Customers with dubious reputation as per public information available or commercially available watch lists
5. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk
6. Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations etc.
7. Customers based in high risk countries/jurisdictions or locations
8. Politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
9. Non-resident customers and foreign nationals
10. Embassies / Consulates
11. Off-shore (foreign) corporation/business
12. Non face-to-face customers
13. High net worth individuals
14. Firms with 'sleeping partners'
15. Companies having close family shareholding or beneficial ownership
16. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
17. Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence
18. Investment Management / Money Management Company/Personal Investment Company
19. Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution.
20. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc.
21. Trusts, charities, NGOs/NPOs (especially those operating on a "cross-border" basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies)
22. Money Service Business: including seller of Money Transmission / Check Cashing /

Currency Dealing or Exchange

23. Business accepting third party cheques (except supermarkets or retail stores that accept payroll cheques /cash payroll cheques)
24. Gambling/gaming including "Junket Operators" arranging gambling tours
25. Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers).
26. Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries.
27. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
28. Customers that may appear to be Multi-level marketing companies etc.

Characteristics of Medium Risk Customers:

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

ANNEXURE – F-3

Indicative List of High / Medium risk Products & Services

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

ANNEXURE – F-4

Indicative List of High / Medium Risk Geographies

Countries/Jurisdictions

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

Locations

1. Locations within the country known as high risk for terrorist incidents or terrorist financing activities (e.g. sensitive locations/cities and affected districts)
2. Locations identified by credible sources as having significant levels of criminal, terrorist, terrorist financing activity.
3. Locations identified by the bank as high-risk because of its prior experiences, transaction history, or other factor

ANNEXURE – F-5

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

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

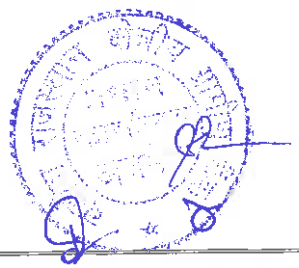
	reporting	to avoid reporting
20.	Customer could not explain source of funds	Customer could not explain source of funds
21.	Transaction is unnecessarily complex	Transaction is unnecessarily complex for its stated purpose
22.	Transaction has no economic rationale	The amounts or frequency or the stated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

ANNEXURE – F-5

Indicative list of Alert Scenarios for Branches/ Departments recommended by IBA working group for detection of suspicious transactions Part- II

S. No.	Code	Alert Indicator
1	WL1.1	Match with UN list
2	WL1.2	Match with UAPA List
3	WL1.3	Match with other TF list
4	WL2.1	Match with other criminal list
5	TM1.1	High value cash deposits in a day
6	TM1.2	High value cash withdrawals in a day
7	TM1.3	High value non-cash deposits in a day
8	TM1.4	High value non-cash withdrawals in a day
9	TM2.1	High value cash deposits in a month
10	TM2.2	High value cash withdrawals in a month
11	TM2.3	High value non-cash deposits in a month
12	TM2.4	High value non-cash withdrawals in a month
13	TM3.1	Sudden high value transaction for the client
14	TM3.2	Sudden increase in value of transactions in a month for the client
15	TM3.3	Sudden increase in number of transactions in a month for the client
16	TM4.1	High value transactions in a new account
17	TM4.2	High activity in a new account
18	TM5.1	High value transactions in a dormant account
19	TM5.2	Sudden activity in a dormant account
20	TM6.1	High value cash transactions inconsistent with the profile of the customer.
21	TM6.2	High cash activity inconsistent with profile
22	TY1.1	Splitting of cash deposits just below INR 10,00,000 in multiple accounts in a month
23	TY1.2	Splitting of cash deposits just below INR 50,000
24	TY1.3	Frequent cash deposits just below INR 10,00,000
25	TY1.4	Routing of funds through multiple accounts
26	TY1.5	Frequent low cash deposits
27	TY1.6	Frequent low cash withdrawals
28	TY2.1	Many to one fund transfer
29	TY2.2	One to many fund transfer
30	TY2.3	Routing of funds through multiple locations
31	TY3.1	Customer providing different details to avoid linkage
32	TY3.2	Multiple customers working together
33	TY4.1	Repeated small cash deposits followed by immediate ATM withdrawals in different location
34	TY4.2	Repeated small value transfers from unrelated parties followed by immediate ATM withdrawals
35	TY4.3	Repeated small value inward remittance from unrelated parties followed by immediate ATM withdrawals
36	TY4.4	Repeated small value withdrawals in sensitive locations
37	TY4.5	Repeated small value inward remittance from unrelated parties used for specified activities
38	TY5.1	Majority of repayments in cash
39	TY5.2	Large debit balance in credit card

40	TY5.3	Large value card transactions for purchase of high value goods
41	TY5.4	Large value cash withdrawals against international card
42	TY5.5	Repeated small value cash withdrawals against international card
43	TY5.6	Large repetitive card usage at the same merchant
44	TY7.1	Repayment of loan in cash
45	TY7.2	Premature closure of large FDR through PO/DD
46	TY7.3	High number of cheque leaves
47	TY7.4	Frequent locker operations
48	RM1.1	High value transactions by high risk customers
49	RM1.2	High value cash transactions in NPO [Non-Profit Organization viz. Trust, Club, Society, NGOs etc.
50	RM1.3	High value cash transactions related to real estate
51	RM1.4	High value cash transactions by dealer in precious metal or stone
52	RM2.1	High value transactions in product/services with high ML risk
53	RM2.2	High value inward remittance
54	RM2.3	Inward remittance in a new account
55	RM2.4	Inward remittance inconsistent with client profile
56	RM3.1	High value transactions with a country with high ML risk
57	RM3.2	High value transactions with tax havens
58	RM3.3	High value transactions in a location with high ML risk
59	RM4.1	Transaction involving a country with high TF risk
60	RM4.2	Transaction involving a location with high TF risk
61	RM4.3	Transaction involving a location with terrorist incident



ANNEXURE – G

Information to be obtained from customer for creating customer profile

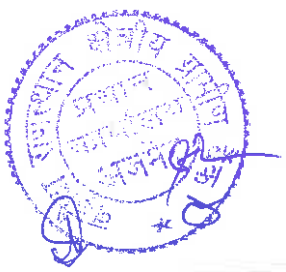
The following information shall be obtained from the customer at the time of account opening for profiling customers based on perceived risk.

Sr. No.	Customer Type	Information to be obtained from customer
1	Individuals	□ Profession- Salaried/ Self- employed □ Annual Income □□If self- employed, nature of profession / business □□Annual turnover in case self- employed supported by Income Tax Returns □ PAN Number
2	Sole Proprietorship	□ Name of Sole proprietor □ Type of business □□Annual turnover supported by Income Tax Returns □□Name and address of Clients (Supplier & Purchaser)
3	Partnership	□ Name of partners □ Type of business □□Annual turnover supported by Income Tax returns □□Name and address of clients (Supplier & Purchaser)
4	Companies	□ Name of directors □ Type of business □□Annual turnover supported by Annual Report □□Name and address of clients (Supplier & Purchaser)
5	Trust, Association, Society, Club etc.	□ Names and addresses of trustees □□Purpose of the such Trust, Association, Society, Club etc. □□Last year's total income supported by Income Tax returns

ANNEXURE – H

Companies/ Individuals identified/ suspected of carrying out MLM activities

1. HIMBJS Holidays Private Ltd.
2. HIMBJS Risk Management Pvt. Ltd.
3. Itech. Eye Consumer Electronic Private Ltd.
4. Spattern Computers Private Ltd.
5. SHIMBJS Automobile Private Ltd.
6. Accresent Way Mktg Pvt. Ltd.
7. Baishag Real Estate and Construction Ltd.
8. Angel Agritech Ltd.
9. Angelay Food Products Pvt. Ltd.
10. Yatra Hospitality Services Pvt. Ltd.
11. SwapnaneerAbasan Pvt. Ltd.
12. Angel Mediline and Research Centers Pvt. Ltd.
13. Angel Rural Development Ltd.
14. Angel Cinivision and Media Pvt. Ltd.
15. Angel Movie Max and Entertainment Pvt. Ltd.
16. Angel Allied India Ltd.
17. Yuvraj Construction
18. MrSekhNazibulla
19. Mr SK HasibulHaque



ANNEXURE – I

Red Flag Indicators for Trade Based Money Laundering Recommended by FIU-IND Working Group

Sr. No.	Red Flag Indicators for Trade Based Money Laundering	Stage
1	Inward remittance followed by immediate withdrawal/ transfer to other accounts	Account
2	Wash sales or round trip sales - Accounts debited and then immediately credited or vice versa for related purchase/ sale	Account
3	Client is involved in high risk or cash intensive business such as money remitting	Account
4	Sudden increase in cash deposits of clients involved in high risk business	Account
5	Use of multiple accounts by customer; or accounts operated for very short period and used for advance remittances only	Account
6	Little or no withdrawal from account for business purposes/ no recurrent business expenses	Account
7	Multiple cash deposits in one country followed by immediate ATM withdrawal in another country	Account
8	Wire transfer accounts opened and closed within a very short period of time	Account
9	Funds received but goods not exported - advance for exports	Advance
10	Funds sent out but good not imported – advance for imports	Advance
11	Advance for supply of goods is a major part/ percentage of the total value of goods	Advance
12	Amount of advance is not in line with normal international trade for the kind of goods	Advance
13	Goods not supplied within reasonable timeframe	Advance
14	Consignment size is unreasonable compared to customer profile/ capacity/ size of business	Consignment
15	Underlying goods involved in the trade transaction are of sensitive nature; trade of similar items by a group of firms from the same overseas supplier (many to one) or vice-versa	Consignment
16	Underlying goods or services not in line with customer's profile and declared business	Consignment
17	Transaction not in-line with normal international trade for the given kind of goods & parties involved	Consignment
18	Transactions related to acquisition or sale of intangibles like PIN, e-codes, specialized software, etc.	Consignment
19	General trading company making payments for purchase of goods that it does not usually purchase/sell/trade in	Consignment
20	High proportion of high seas sales/ merchanting trades	Consignment
21	Transactions involving third parties which may not be contract parties (consignee and remitter are different)	Counterparties
22	Payments/fund transfers made through economic/exchange centers even when account is held with financial institutions	Counterparties
23	Related party transactions including transfer pricing	Counterparties

231.

Sr. No.	Red Flag Indicators for Trade Based Money Laundering	Stage
24	Unknown counterparties to a trade transaction	Counterparties
25	Non-resident's payments to companies/natural persons who have accounts with offshore Banks	Counterparties
26	Trade activity done from port which is far from the importer/exporter's base location. Example importer is in Surat and goods imported through a remote port in Assam	Location
27	Description of goods provided is vague	Documentation
28	Prima facie the documents submitted look suspicious	Documentation
29	Substantial inconsistencies between the information originally supplied and that contained in the documents	Documentation
30	Suspected discrepancies between description of goods on transport document vis-à-vis invoice/other documents	Documentation
31	Unnecessarily complex transactions that lack economic sense	Documentation
32	Over/under/multiple invoicing, apparently suspect (apparently fraudulent/fake) documents	Documentation
33	Export/import documents are not submitted and account behavior of the customer appears to be suspicious	Documentation
34	Import payments being made against old bills after lapse of considerable period of time from import of goods, without appropriate justification and documentation	Documentation
35	Remittances to or from high risk jurisdictions	Jurisdiction
36	Goods transshipped through high risk jurisdictions for no apparent reason	Jurisdiction
37	Circuitous route of shipment/shipment of goods inconsistent with normal geographic trade	Jurisdiction
38	Amounts of money transfer carried out by natural persons and legal entities are multiples of 100/1,000/10,000/100,000 USD /EUR / National currency	Payment
39	Originator's bank uses cover payment when wiring funds to beneficiary's bank	Payment
40	Originator of transfer not able to provide documents on source of the money	Payment
41	Structuring of transactions to avoid threshold reporting	Payment
42	Structuring of transactions to avoid submission of BOE (Remittance amounts kept just below the threshold of USD 100,000 or equivalent value)	Payment
43	Customer selling items on a commercial website and receiving money via internet payment service provider	Payment
44	Originator/beneficiary information missing in wire transfers	Payment
45	Foreign currency exchange transactions by non-residents over a short period of time where transfers are affected through non-banking remittance systems	Payment
46	Use of repeatedly amended or frequently extended letters of credit without reasonable justification or for reasons like changes of beneficiary or location	Payment
47	Accounts funded by negotiable instruments (such as travellers' cheques, cashier's cheques, etc.) in round denominations	Account
48	Importer of goods not from the same country from where wire (payment for import) originated	Counterparties

Sr. No.	Red Flag Indicators for Trade Based Money Laundering	Stage
49	Foreign based importing entity with accounts in exporting country receiving payments from locations outside the area of its customer base	Counterparties
50	Packing inconsistent with the commodity or shipping method	Consignment
51	Carousel transactions – repeated importation and exportation of same high-value commodity	Consignment
52	Service locations or description of services that are inconsistent with the letter of credit	Services
53	Booking of ticket abroad and subsequent cancelling and payment made to third party.	Services
54	Hiring of services which are not in accordance with company Requirement.	Services
55	Forex for medical treatment as per prescribed limit but availed multiple times from multiple ADs.	Services
56	Value and/or total quantity of goods is not easily ascertainable	Valuation
57	Significant discrepancies appear between the value of goods or services reported on the invoice and fair market value	Valuation
58	A customer deviates significantly from its historical pattern of trade activity (i.e. in terms of markets, monetary value, frequency of transactions, volume, or merchandise type)	Account
59	Transacting parties appear to be affiliated, conduct business out of a residential address, or provide only a registered agent's address	Customer
60	The LC contains non-standard clauses or phrases or has unusual characteristics	Documentation
61	LC contains non-standard clauses or phrases or has unusual characteristics	Payment
62	Payment terms or tenor are inconsistent with the type of goods	Documentation
63	Frequent change in payment instruction at the last minute	Payment