KYC / AML Policy – 2025-26

Amended/ updated up to 06.11.2024

KYC / AML Cell

Planning, Development & Operations Department

CENTRAL OFFICE

"All related statutory guidelines/ circulars issued by RBI/ GOI are incorporated in the policy. Further, if any amendments to the existing norms are made by the Reserve Bank of India or other Statutory Bodies/ Regulators, the same will be applicable and it will be treated as part of the policy."

Preface

Our previous KYC / AML Policy 2024-25 (updated upto 04.01.2024) was circulated to the Branches vide Circular No. 3942 for its implementation on 30th March, 2024, wherein we have incorporated amendments notified by Reserve Bank of India (RBI) to its Master Direction - Know Your Customer (KYC) Direction, 2016 till 04.01.2024.

In terms of the provisions of PML Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India as notified by the Government of India, Banks being Regulated Entities (REs) are required to follow certain customer identification procedures and conduct customer due diligence while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions and take steps to ensure implementing the provisions of the aforementioned Act, Rules and Ordinance, including operational instructions issued in pursuance of such amendment(s).

We are now presenting the updated Policy incorporating amendments notified by Reserve Bank of India **till 06.11.2024** in its Master Direction - Know Your Customer (KYC) Direction, 2016 for implementation before the field functionaries such as Branches/ Regional offices/ Zonal offices/ Central Office Departments for guidance and compliance while on boarding customers and as well as during the conduct of the accounts.

We trust the various procedures laid down in the policy will be scrupulously followed to avoid pitfalls and to prevent use of banking channels for money laundering, financing terrorism and proliferation of Weapons of mass-destruction activities.

We confirm that all related statutory guidelines/ circulars issued by RBI/ Govt. of India have been incorporated in the Policy.

Branches/ Regional Offices / Zonal Offices are also advised to refer any further directions / guidelines/ Circulars / Policy amendments issued by the departments and Regulatory Authorities from time to time on KYC.

-Sd-
(KUSHAL PAL)
GENERAL MANAGER – CCD

01.03.2025
Place: Mumbai

KYC - AMLPolicy-2023-24 (updated upto 06.11.2024)

INDEX

POLICY/GUIDELINES ON 'KNOW YOUR CUSTOMER' (KYC) NORMS AND ANTI MONEY LAUNDERING MEASURES.

1. "KNOW YOUR CUSTOMER" NORMS.

1.1. Know Your Customer (KYC) is the platform on which Banking System operates to avoid the pitfalls of operational, legal and reputation risks and consequential losses by scrupulously adhering to the various procedures laid down for opening and conduct of account.

1.2. Know Your Customer is the key principle for identification of any individual/corporate opening an account.

1.3. The customer identification should entail verification on the basis of documents provided by the customer. The objectives of KYC are as under:

1.3.1. To ensure appropriate customer identification.

1.3.2. Monitor the transactions of a suspicious nature.

1.3.3. Obtaining protection Under Section 131 of Negotiable Instruments Act.

1.3.4. Minimize the risk due to any inadvertent overdraft.

1.3.5. Satisfy that the proposed customer is not an un-discharged insolvent.

1.3.6. Minimize frauds.

1.3.7. Avoid opening of Benami account/accounts with fictitious name and addresses and

1.3.8. Weed out undesirable customers.

1.4. For the purpose of KYC policy a "Customer" means

1.4.1. A person or entity that maintains an account and/or has a business relationship (engaged in financial transaction or activity)with the Bank including walk-in customers.

1.4.2. One on whose behalf the account is maintained (i.e. the beneficial owner).
The term "beneficial owner" has been defined as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person.

The procedure for determination **of Beneficial Ownership** is as under:

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

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

Explanation: - For the purpose of this sub clause-
"Controlling ownership interest" means ownership of/entitlement to more than **Ten percent (10%)** of 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 10 percent of capital or profits of the partnership or who exercises control through other means.

Explanation - For the purpose of this sub-clause, "control" shall include the right to control the management or policy decision.

(c) Where the client is an unincorporated association/ Society 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 or entitlement to more than fifteen percent (15%) of the property or capital or profits of such unincorporated association or body of individuals;

Explanation: Term 'body of individuals' includes societies.

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 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 Ten percent (10%) or more interest in the Trust and any other natural person exercising ultimate effective control over the Trust through a chain of control or ownership.

e) Exemption from Identification of Beneficial Owner: The exemption from BO identification has been aligned with that provided in the PML Rules, 2005, such that where the customer or the owner of the controlling interest is
(i) an entity listed on a stock exchange in India, or
(ii) an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or
(iii) a subsidiary of such listed entities;
In such cases, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such an entity.

i) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases,

satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

1.4.3. Beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers, Chartered Accountants, Solicitors etc., as permitted under the law and

1.4.4. Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

1.4.5.As per the instructions of RBI vide their letter No. DoS.CO.RPG/ 3923/ 11.01.002/ 2002/ 2019-20 dated December 20, 2019 as per Section 3 (a) (iv) of the Master Direction- Know Your Customer (KYC) Direction, 2016 and also the Rule 9(1)(a) of the PML (Maintenance of Records) Rules 2005, further in terms of amendments to PML rules carried out by Govt. of India in August 2019, Beneficial Owner once established, has to be identified in the same manner as an individual customer. Thus Banks are required to identify the beneficial owner and take all reasonable steps to verify his identity.

1.4.6. Further, RBI advised that FATF Recommendation 10(b) on AML/ CFT and the FATF [paper on the best Practices on Beneficial Owner ship for legal Persons (October 2019), available on the website of FATF (http://www.fatf-gafi.org/), may be referred to for further guidance on the identification of BO.

1.4.7. Branches are advised to follow the extent regulatory provisions in respect of identification of BO and establishing relationship of Legal entity customers with BO while establishing account based relationship with entity customers. Branches shall ensure that KYC documents of Beneficial owner, as per extant requirements of Master Direction are obtained, verified from the verification facility of the issuing authority and are available on record with them.

1.4.8. For the KYCAML compliances, the term "Group" shall have the same meaning assigned as per Income tax act-1961, under clause (e) of sub-section (9) of Section 286, which is defined as under.

"Group includes a parent entity and all the entities in respect of which, for the reason of ownership or control, a consolidated financial statement for financial reporting purposes, (i) is required to be prepared under any law, for the time being in force, or the accounting standards of the country or territory of which the parent entity is resident or

(ii) Would have been required to be prepared had the equity shares of any of the enterprises were listed on a stock exchange in the country or territory of which the parent entity is resident."

(a). The Bank shall have "Know Your Customer (KYC) policy" duly approved by the Board of Directors or any committee of the Board to which power has been delegated.

(b). In terms of PML Rules, groups are required to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the PML Act, 2002. (15 of 2003).Accordingly, every Reporting Entity, which is part of a group, shall implement group-wide programmes against money laundering and terror financing, including group-wide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management and such programmes shall include adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

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

2. CUSTOMER ACCEPTANCE POLICY (CAP)

2.1 ACCOUNT OPENING PROCEDURES

2.1.1. Any Indian National-resident / Non-resident / Partnership firms / companies / Trusts/ un-incorporated associations or Body of Individuals, etc., can open an Account with a Bank either singly or jointly with other.

2.1.2 The prospective account holder has to complete the following formalities before the bank account can be made operational:-

2.1.2.1 Since introduction is not necessary for opening of accounts under PML Act and Rules or Reserve Bank's extant KYC instructions, branches should not insist on introduction for opening bank accounts of customers, when documents of identity & address, as required, are provided.

2.1.2.2 The provisions for opening of 'Small Accounts' with introduction from an existing accountholder or other evidence of identity and address to the satisfaction of the bank were made to help persons who were not able to provide 'officially valid documents' for opening of accounts. In view of the said provisions for 'Small Accounts' being included in sub-rule (5) of rule 9 of the PML Rules, the extant instructions for opening of 'Accounts with Introduction' as earlier prescribed stands withdrawn.

Small Account' means a saving account in a banking company where:-

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

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

(a) A 'small account' may be opened on the basis of a self-attested photograph and affixation of signature or thumb print. Such accounts may be opened and operated subject to the following conditions:

i) the designated officer of the branch, while opening the small account, certifies under his signature that the person opening the account has affixed his signature or thumb impression, 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.

i) A small account shall be 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.

ii) The stipulated limits on monthly and annual aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place;

iii) A small account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence to the branch of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months;

iv) A 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 customer shall be established through the production of aadhaar or any "officially valid documents" or the equivalent e-document thereof containing the details of identity and address and PAN or equivalent e-document thereof or Form 60; and

v) Foreign remittance shall not be allowed to be credited into a small account unless the identity of the customer is fully established through the production of Aadhaar or any "officially valid documents" or the equivalent e-document thereof containing the details of identity and address and PAN or equivalent e-document thereof or Form 60.

vi) The prescribed limits / conditions shall not be breached and compliance therewith shall be strictly monitored. If any customer desires to have operation beyond the stipulated limits, the same can be allowed only after complying with the requirements for opening a normal account including quoting of PAN or equivalent e-document thereof or Form 60.

vii) If any account is rendered ineligible for being classified as a small account due to credit /balances in the account exceeds the permissible limits, withdrawals may be allowed within the limit prescribed for small accounts where the limit thereof have not been breached.

2.1.2.3 Submit 2 recent passport sized photographs for affixing them to the account opening form and specimen signature card/pass book.

2.1.2.4 Provide specimen signature in the presence of a verifying official.

2.1.2.5 Indicate mode of operation.

2.1.2.6 Avail of the nomination facility in case of individual accounts.

2.1.2.7 Provide documents for identification and proof of residence - Particulars of present or permanent addresses along with telephone numbers/fax/ email etc. if installed or any contact telephone number. Provided that:

a. If the address on the document submitted for identity proof by the prospective customer is same as that declared by him/her in the account opening form, the document may be accepted as a valid proof of both identity and address.

b. If the address indicated on the document submitted for identity proof differs from the address mentioned in the account opening form, a separate proof of address should be obtained.

Henceforth, customers may submit only one documentary proof of address (either current or permanent) while opening a bank account/ while under-going periodic updation. In case the address mentioned as per 'proof of address' undergoes a change, fresh proof of address may be submitted to the branch within a period of six months.

In case the proof of address furnished by the customer is not the local address or address where the customer is currently residing, the branch is to merely take a declaration of the local address on which all the correspondence will be made by the branch with the customer. No proof is required to be submitted for such address for correspondence/local address. This address may be verified by the bank through 'positive confirmation 'such as acknowledgement of receipt of (i) letter, cheque-books, ATM cards; (ii) telephonic conversation;(iii) visits; etc. In the event of change in this address due to relocation or any other reason, customers may intimate the new address for correspondence to the bank within two weeks of such a change.

If the address provided by the account holder is the same as that on Aadhaar letter issued by UIDAI, it may be accepted as a proof of both identity and address. NREGA Job Card may be accepted as an 'officially valid document' for opening of bank accounts without the limitations applicable to 'Small Accounts'.

2.1.2.8 Give details of other accounts with any other banks

2.1.2.9 Permanent Account Number (PAN) given by Income Tax authorities or equivalent e-document thereof of customers shall be obtained. Verification of PAN number should be done online from system/Income Tax site as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN or equivalent e-document thereof.

2.1.2.10 Registration Certificate in case of proprietorship concern/partnership firms and Certificate of Incorporation, Memorandum and Articles of Association, Resolution by Boards for accounts of Companies.

2.1.2.11 **Simplified KYC norms for Foreign Portfolio Investors (FPIs):**

Eligible/registered FPIs with SEBI may approach a branch for opening an account for the purpose of investment under Portfolio Investment Scheme (PIS) for which KYC documents prescribed by the Reserve Bank would be required as detailed in Annexure V subject to Income Tax (FATCA / CRS) Rules. Branch shall obtain undertaking from FPIs or the Global Custodian acting on behalf of the FPI that as and when required, the exempted documents as detailed in Annexure V will be submitted.

2.1.2.12 **Foreign students studying in India– KYC procedure for opening of bank accounts:**

a) Foreign students arriving in India, who are not able to provide an immediate address proof while approaching a bank for opening bank account may be allowed to 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.

b) Within a period of 30 days of opening the account, the foreign student should submit to the branch where the account is opened, a valid address proof giving local address, in the form of a rent agreement or a letter from the educational institution as a proof of living in a facility provided by the educational institution and the said local address is to be verified.

c) During the 30 days period, the account should be operated with a condition of allowing foreign remittances not exceeding USD1,000 or equivalent into the account and a cap of monthly withdrawal to Rs.50,000/- on aggregate, pending verification of address.

d) On submission of the proof of current address, the account would be treated as a normal NRO account and will be operated in terms of the instructions contained in RBI's instructions on Non-Resident Ordinary Rupee (NRO) account and the provisions of FEMA 1999.

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

2.1.2.13 Copies of the submitted KYC documents must be verified with the originals and officials accepting such documents should invariably put a stamp "Original seen and verified" (OSV stamp) under her/his signature, name, index number and date.

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

2.1.2.14 Revised norms for Self Help Group–KYC procedure/ CDD for opening of bank accounts

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

2.1.2.15 Additional information, where information requirement has not been specified in the internal KYC Policy of the Bank, is obtained with the explicit consent of the customer. Where GST number is available, the same shall be verified through the search/verification facility provided by the issuing authority.

2.1.2.16 Branch has to ensure that KYC documents downloaded from the CKYCR, but whose validity has lapsed, are not used for KYC purpose by the downloading Branch **.**

2.1.3 The above documents/data would help to establish the identity of the person opening the account, but would not be sufficient to prepare a profile of expected activities in the account. Towards this, the following additional details need to be collected while opening the account:

2.1.3.1.Employment details such as job specifications, name and address of the employer, length of service, etc.

2.1.3.2. Provide details about source of income and annual income.

2.1.3.3. Details of assets owned such as house, vehicle etc.

2.1.3.4. Other personal details such as qualification, marital status, etc.

2.1.3.5. It is to be ensured that the additional information sought from the customer is relevant to the perceived risk, is not intrusive and is in conformity with the guidelines issued in this regard.

2.1.3.6 A list of Do's and Don'ts on KYC Norms and AML Standards is enclosed as Annexure II.

(The information obtained from the customers at the time of opening of account should not be used for cross selling purposes. The additional information/details for preparing the customer profile may be collected with the express approval of the

customer and that such information should not form part of account opening form. Separate customer profile should be prepared).

2. PRECAUTIONS TO BE TAKEN

While opening the account it should be ensured that:-

2.2.1. No account is opened in anonymous or fictitious/ Benami name(s).

2.2.2. No account should be opened where the bank is unable (to verify the identity and/or obtain documents required or non-reliability of the data/information furnished to the bank) to apply appropriate CDD measures, either due to non - cooperation of the customer or non-reliabity of the documents/ information furnished by the customer. The Bank shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.

2.2.3 No transaction or account - based relationship is undertaken without following CDD procedure.

2.2.4. Before opening a new account, it should be ensured 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. The Branches should refer the circulars issued by RBI/Government of India/Central Office from time to time where in the names of banned/terrorist individuals/organization etc. are notified. The name(s) of the prospective customer should be verified with the latest "List of Terrorist Individuals/Organization under UNSCR 1267(1999) and 1822(2008) on Taliban/Al-Qaida Organization" integrated with CBS for 100% match and for more than 90% match available at Bank's ftp server and the path -ftp://centftp.cbi.co.in/public/aml.

2.2.5. In cases where the customer is permitted to act on behalf of another person/entity the circumstances should be clearly spelt out 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 may be opened by an intermediary in the fiduciary capacity.

2.2.6 Risk Categorization of Customers: Customers shall be categorized as low, medium and high risk category, based on the assessment and risk perception. The branches should prepare the profile of the customer which should contain information relating to customers' identity, social/financial status, nature of business activity, information about his clients' business and their location etc. and risk categorization shall be undertaken based on these parameters. While considering customer's identity, the ability to confirm identity documents through online or other services offered by the issuing authorities may also be factored in. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposeswithout the express permission of the customer.

2.2.7 The customer profile shall be prepared based on risk categorization, as detailed in Para: 9 of this Policy.

2.2.7.1 Branch may take a view on risk categorization of each customer into low, medium and high risk category depending on their experience, expertise in profiling of the customer based on their understanding, judgment, assessment and risk perception of the customer and not merely based on any group or class they belong to.

2.2.7.2 There should be periodical review of risk categorization of accounts followed by enhanced due diligence measures. Such review of risk categorization of customers should be carried out at least once in every six months.

2.2.8 It should be noted that Banking Services are not denied to general public, especially to those who are financially or socially disadvantaged.

Explanation: FATF Public statement, the reports and guidance notes on KYC/AML issued by the Indian Bank Association (IBA) may also be used in risk assessment.

2.2.**9** Compliance with the provisions of Foreign Contribution (Regulation) Act, 2010

Banks shall ensure adherence to the provisions of Foreign Contribution (Regulation) Act, 2010 and Rules made thereunder. Further, banks shall also ensure meticulous compliance with any instructions / communications on the matter issued from time to time by the Reserve Bank based on advice received from the Ministry of Home Affairs, Government of India.

3. CUSTOMER IDENTIFICATION PROCEDURE (CIP)

One of the objectives of the "KYC" norms is to ensure appropriate Customer Identification. Customer Identification means undertaking the process of Customer due diligence (CDD)i.e. identifying the customer and verifying his/her identity by using reliable, independent source of documents, data or information.

Customer identification procedure is to be carried out at different stages i.e.

a. While establishing a banking relationship i.e. commencement of an account-based relationship with the customer.
b. carrying out a financial transaction/ international money transfer operations for a person who is not an account holder of the Bank.
c. When the bank has a doubt about the authenticity / veracity or the adequacy of the earlier obtained customer / identification data.
d. Carrying out any international money transfer operations for a person who is not an account holder of the bank.
e. Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than fifty thousand.
f. Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
g. When there is reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
h. Bank shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business, risk profile and the source of funds / wealth.
i. Provided that in case of a trust, the Bank shall ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in clauses (b), (f) and (g) as above.

Branches need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship. Being satisfied means that we are able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.

3.1 IDENTIFICATION OF CUSTOMER

Identification of a customer is an important pre-requisite for opening an account. No Account is opened for any person without proper verification of the identity of the person. Careless handling of the matter may give room for undesirable customers to commit frauds, misappropriation and deceive the general public. Necessary precaution and strict adherence of norms in this respect can be a check on the activities of miscreants trying to defraud the Banking System.

Video based Customer Identification (V-CIP) is an alternate method of customer identification with facial recognition and customer due diligence by an authorized official of the branch for opening an account by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such process complying with prescribed standards and procedures shall be treated on par with CIP process.

3.1.1 WHAT IS IDENTITY?

Identity generally means a set of attributes which together uniquely identify a' natural' or a 'legal' person. The attributes which help in unique identity of a' natural' or 'legal' person are called "identifiers". Identifiers are of two types: (A) Primary and (B) Secondary.

A) Primary Identifiers : Means and includes name (in full), Father's name, Date of Birth, Passport number, Voter Identity Card, Driving License, PAN number etc. as they help in uniquely establishing the identity of the person.

B) Secondary Identifiers: Includes address, location, Nationality and other such identification, as they help further refine the identity. The customer identification does not start and end at the point of application but it is always an ongoing exercise.

3.1.1.1. **Natural Person:** A natural person's identity comprises his name andall other names used, the date of birth, and an address/location at which he/she can be located and also his/her recent photograph.
3.1.1.2. **Legal Person:** The legal status of the legal person/entity should be verified through proper and relevant documents; verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person; understand the ownership and control structure of the customer and determine who are the natural person(s) who ultimately control the legal person.

The identity of a legal/corporate person comprises its name, any other names it may use, and details of its registered office and business addresses.

3.1.2 WHAT IS IDENTIFICATION?

3.1.2.1. Identification is the act of establishing who a person is.

3.1.2.2. In the context of KYC, identification means establishing who a person purports to be.

3.1.2.3. This is done by recording the information provided by the customer covering the elements of his identity (i.e. name and all other names used, and the address at which they can be located).

3.1.2.4. For undertaking CDD, the following shall be obtained 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. The features to be verified and the documents to be obtained for establishing identity of a person/customer are as under:-

Features	Documents
Accounts of Individuals •Legal name and Any other names used •Correct permanent address	A. Permanent Account Number (PAN) or the equivalent e-document there of or Form No. 60 as defined in Income-tax Rules, 1962, as amended from time to time and such other documents including in respect of financial status of the customer, or the equivalent e-documents thereof as may be required along with: where PAN is obtained, branches should verify the PAN from the verification facility of the issuing authority (NSDL). B. Certified copy of any "Officially Valid Document" (OVD) or the equivalent e-document thereof containing the details of identity and address. **"Officially Valid Document" (OVD) means** i) the passport, ii) the driving license, iii) proof of possession of Aadhaar number, iv) the Voter's Identity Card issued by the Election Commission of India, v) job card issued by NREGA duly signed by an officer of the State Government and vi) Letter issued by the National Population Register containing details of name and address. vii) CKYC identifier number.

	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 v. Leave and license agreements with such employers allotting official accommodation; c. Provided that the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above The additional documents mentioned above shall be deemed to be OVDs for the 'low risk' customers for the limited purpose of proof of address, where customers are unable to produce any OVD for the same. d. From an individual who is not a resident, PAN or Form No. 60 as defined in Income-tax Rules, 1962, as amended from time to time and a certified copy of an OVD containing details of identity and address shall be obtained. In case the 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 shall be accepted as proof of address. e. A document shall be deemed to be an 'Officially Valid

	Document' 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 a Gazette notification indicating such a change of name, while establishing an account based relationship or during periodic updation exercise, for persons whose name is changed due to marriage or otherwise. **When Aadhaar number is received from customers,** 1) Branches may carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India (UIDAI) 2) Provided that in cases where successful authentication of Aadhaar number using e-KYC facility has been carried out, the other OVDs and photograph need not be submitted by the client. 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 branch. 3) The branch shall carry out offline verification where offline verification can be carried out on the proof of possession of Aadhaar. "Offline verification" means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the regulations of UIDAI. Where customers submits his Aadhaar number, branches to ensure such customers to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required. For equivalent e-document of any OVD, the branches shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues there under and take a live photo as specified under Annex I. Any OVD or proof of possession of Aadhaar number where offline verification cannot be carried out, the branch shall carry out verification through digital KYC as specified under Annex I. Provided that for a period not beyond such date as may be notified by the Government, instead of carrying out digital KYC, the branches may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e -document is

	not submitted. Provided further that in case e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, branches 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 branch and such exception handling will also be a part of the concurrent audit as mandated in M D of RBI that Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures. Branches shall ensure to duly record the cases of exception handling in a centralized exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorizing 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.
Accounts of Companies •Name of the Company •Principal place of Business. •Mailing address of the company •Telephone/Fax Number	For opening an account of a company, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained: a) Certificate of incorporation; b) Memorandum and Articles of Association; c) Permanent Account Number of the Company d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and e) Documents specified for CDD procedure for individuals includes obtaining Aadhaar or any officially valid document or the equivalent e-document thereof containing the details of proof of identity and address, one recent photograph and Permanent Account Number (PAN) or the equivalent e-document thereof or Form 60relating to the beneficial owner, the managers or employees as the case may be, holding an attorney to transact on the company's behalf. f). CST/VAT/GST certificate (provisional/final). Branches should search/ verify the GST number from the verification facility of the issuing authority (g) the names of the relevant persons holding senior management position; and **(**h) the registered office and the principal place of its business, if it is different.

Accounts of Proprietorship concerns:	For opening an account in the name of sole proprietary firm, CDD of the individual (proprietor) shall be carried out and includes obtaining Permanent Account Number (PAN) or the equivalent e-document thereof or Form 60, one recent photograph and Aadhaar or Officially valid document or the equivalent e-document thereof containing the details of proof of address and proof of identity of the individual proprietor along with Certified copies of any two of the following or the equivalent e-documents thereof as a proof of business / activity in the name of the proprietary firm : 1. Proof of name, address and activity of the concern like Registration Certificate (In the case of registered concern). 2. Certificate/license issued by Municipal Authorities under Shop & Establishment Act. 3. Utility bills such as electricity, water and landline telephone bills in the name of the proprietary concern. 4. Sales return and income tax Returns. 5. The complete Income tax return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax Authorities. 6. CST/VAT/GST certificate (provisional/final). Branches should search/verify the GST number from the verification facility of the issuing authority. 7. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. 8. Registration/licensing document issued in the name of the proprietary concern by the Central Government or State Government authority/Departments *includes "Udyam Registration Certificate (URC)" issued by the Government*. 9. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/License /certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute as an identity document for opening of bank account. It has been clarified that though the default rule is that any two documents should be provided as activity proof, in case where the Branch is satisfied that it is not possible to furnish two such documents, then it will have the discretion to accept only one of the specified documents as activity proof. However the Branch will have to undertake contact point verification and collect such information and clarification as would be required to establish the existence of such firm and confirm, clarify and satisfy itself that the business activity has been verified from the address of the proprietary concern. After proper verification of the business activity and the address of the proprietary concern, a physical record of the contact point verification should be maintained along with the other KYC documents.. It is further clarified that the list of registering authorities indicated

	above are only illustrative and therefore will also include license/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under the statute as one of the documents to prove the activity of the proprietary concern.
Accounts of Partnership firms	For opening an account of a partnership firm the certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained: a) Registration certificate; b) Partnership deed; c) Permanent account number of the partnership firm and d) Documents specified for CDD procedure for individuals and includes obtaining aadhaar or any officially valid document or the equivalent e-document thereof containing the details of proof of identity and address, one recent photograph and Permanent Account Number (PAN) or the equivalent e-document thereof or Form 60relating to the beneficial owner, the managers, officers or employees as the case may be, holding an attorney to transact on its behalf. e) CST/VAT/GST certificate (provisional/final). Branches should search/ verify the GST number from the verification facility of the issuing authority (f) the names of all the partners; and (g) address of the registered office, and the principal place of its business, if it is different.
Accounts of Trusts, & Foundations	For opening an account of a trust, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained, **apart from disclosure of status and names of the Trustees at the time of commencement of an account-based relationship or when carrying out transactions.** a)Registration certificate, b)Trust deed, c) Permanent account number or Form 60 of the trust; d) Documents specified for CDD procedure for individuals and includes obtaining aadhaar or any officially valid document or the equivalent e-document thereof containing the details of proof of identity and address, one recent photograph and Permanent Account Number (PAN) or the equivalent e-document thereof or Form 60relating to the beneficial owner, the managers, officers or employees as the case may be, holding an attorney to transact on its behalf. (e) the names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust. **(**f) the address of the registered office of the trust; and (g) list of trustees and documents, as specified in Section 16, for those discharging role as trustee and authorized to transact on behalf of the

	trust. h) DARPAN ID generated on the DARPAN Portal of NITI Aayog, provided if the Trust/ Foundation is constituted for religious or charitable purposes referred in clause (15) of section 2 of the Income-Tax Act, 1961 and registered under Societies Registration Act,1860 or any similar state legislation or a Company registered under Section -8 of the Companies Act, 2013.
Unincorporated Association or Body of Individuals	For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained: a) Resolution of the managing body of such association or body of individuals; b)Permanent account number or Form 60 of the unincorporated association or a body of individuals; c) Power of attorney granted to him to transact on its behalf; d) Documents specified for CDD procedure for individuals and includes obtaining aadhaar or any officially valid document or the equivalent e-document thereof containing the details of proof of identity and address, one recent photograph and Permanent Account Number (PAN) or the equivalent e-document thereof or Form 60relating to the beneficial owner, managers, officers or employees as the case may be, holding an attorney to transact on its behalf. and e) Such information as may be required by the branch to collectively establish the legal existence of such an association or body of individuals. *Explanation: Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'.* *Explanation: Term 'body of individuals' includes societies.*
Juridical Persons: Government or its departments, Universities and Local bodies like Village Panchayats	For opening accounts of juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents or the equivalent e-documents thereof shall be obtained: a) Documents showing name of person authorized to act on behalf of the entity; b) Documents specified for CDD procedure for individuals and includes obtaining aadhaar or any officially valid document or the equivalent e-document thereof containing the details of proof of identity and address, one recent photograph and Permanent Account Number (PAN) or the equivalent e-document thereof or Form 60 relating to the beneficial owner, managers, officers or employees as the case may be, holding an attorney to transact on its behalf and c) Such documents as may be required by the branch to establish the

	legal existence of such an entity / juridical person.
Customer Identification & CDD measures for opening of accounts of Society.	Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained: 1. Registration certificate issued by Register of Societies 2. Society Bye-Laws duly signed by Office Bearer, Competent Authority. 3. Resolution with operating Instructions issued by the Society. 4. PAN OR Exemption certificate (12A) under Sec 80G of IT Act. 5. DARPAN ID generated on the DARPAN Portal of NITI Aayog, provided if the society is constituted for religious or charitable purposes referred in clause (15) of section 2 of the Income-Tax Act, 1961 and registered under Societies Registration Act,1860 or any similar state legislation or a Company registered under Section -8 of the Companies Act, 2013. In addition to this all documents, branches are required to obtain the KYC documents of the Beneficial owner, the Managers, Officers or employees as the case may be, holding an attorney/ Authority to transact on its behalf as applicable to individual Customers.
Customer Identification & CDD measures for opening of accounts of Hindu Undivided Family (HUF)	Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained: 1. Proof of Identity & Proof of Address of Karta (any of the OVD or equivalent e-document) 2. Permanent account number of the HUF or Form 60; 3. Permanent account number of the Karta or Form 60. **4.** Karta Declaration form along with details of coparceners of HUF.

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

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: a) authorized officials of overseas branches of Scheduled Commercial Banks registered in India, b) branches of overseas banks with whom Indian banks have relationships, c) Notary Public abroad, d) Court Magistrate, e) Judge, f) Indian Embassy/Consulate General in the country where the nonresident customer resides.

3.1.2.5 **Salaried Persons:**

An account should not be opened, for salaried employees, by relying on a certificate/letter issued by the employer as the only KYC document for the purposes of certification of

identity as well as address proof. Such a practice is open to misuse and fraught with risk. Branches should insist on PAN along with documents specified for CDD procedure in case of individuals to open account of salaried employees of corporate and other entities.

3.1.2.6 **Full operational facilities in with spouse staying at separate stations:**

Branches may consider extending full operational facilities, like issuance of ATM/Debit Card, mobile banking, purchase of DD, transfer of funds, utility bill payments, merchandising services, purchases etc. by using 'on-line' banking facility, to the spouse staying at different stations, if one of them i.e. husband or wife is staying at home-branch station.

3.1.2.7 **Accounts portability/ opening of new Bank Accounts:**

Branches are advised that KYC once done by one branch should be valid for transfer of the account within the bank as long as full KYC verification has been done for the concerned account and the same is not due for periodic updation. The customer should be allowed to transfer his account from one branch to another branch without restrictions. Branches may transfer existing accounts at the transferor branch to the transferee branch without insisting on fresh proof of address.

Bank shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer desires to open another account **or avail any other product or service from any branch of our Bank,** there shall be no need for a fresh CDD exercise **as far as identification of the customer is concerned.**

3.1.2.8 **Accounts of Politically Exposed Persons (PEPs):**

A. "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions **by a foreign country**, including the Heads of States / Governments, senior politicians, senior government or judicial or military officers, senior executives of state owned corporations and important political party officials.

Explanation for the above definition is as under:

1. PEP is any Individual or official who are or have been entrusted with prominent public functions in a foreign country such as Foreign secretary or Joint Secretary or ambassadors, mission officials working at Indian Embassies situated in Foreign country or Multilateral organizations or Vice versa.
2. Heads of states includes President, Vice-President & Prime Minister of the country and Governors & Chief Ministers of all states.
3. Senior politicians includes All Ministers at Centre and State Governments, Members of Parliament (both Lok-Sabha & Rajya-sabha), Members of State Legislative Assemblies/ Councils (MLAs & MLCs),

4. Senior Government Officials includes Officials recruited through all India Services and appointed as heads/ secretaries/ joint secretaries at various Central & state Government Departments.
5. Senior Judicial Officials include all Judges appointed at Supreme Court and High Courts in India.
6. Senior military Officials include all senior level officers appointed as head/ Chief of all defence services including military, navy & Air-force.
7. Senior executives of state owned corporations include all Chairpersons and Managing Directors appointed to Various Corporations sponsored by Central & State Governments.
8. Important political party officials include Individuals elected to or appointed by political parties, which are recognised by Election Commission of India or respective State Election Commissions, as President, Vice President, General Secretary, Joint Secretary, Treasurer, Spokesperson and members of Central and State level committees of Recognised Political Parties.

The identity of the person is to be verified before accepting PEP as the customer. The decision to open an account for PEP should be taken at a senior level at Regional Office.

B. While establishing an Account based relationship with PEPs, (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence the branches should ensure to obtain the following information on the PEP :

i. Bank has to put in place an appropriate risk management systems to identify/ determine whether the customer or the beneficial owner is a PEP;

ii. Branches should take Reasonable measures for establishing the source of funds / wealth;

iii. sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;

iv. the identity of the person shall have been verified before accepting the PEP as a customer;

v. the decision to open an account for a PEP is taken at a senior level say at Regional Office as per 'Customer Acceptance Policy' of the Bank. For this purpose, Branch Manager in case of Scale IV and above Branches and Regional Managers in case of Branches up to Scale III are the competent authority to take decision to open an account of PEPs.

vi. all such accounts are subjected to enhanced monitoring on an on-going basis;

vii. 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;

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

C These instructions shall also be applicable to accounts where PEP is the beneficial owner, family member or close associate of PEP.

3.1.2.9 High Net-worth Individuals/ Customers (HNIs):

High net Worth Individual (HNI) is a term used by financial services Industry (Banks/ FIs) to designate Individual Customers whose investible wealth exceeds a given amount. Typically these individuals are defined based on holding of financial assets value greater than some amount to be decided by the concerned Financial Institution/ Banks.

The 'High net-worth Individuals (HNIs)' are defined as those Individual customers who fulfills any one of the following two criteria and shall be categorized as High Risk Customers.

A) Average Account Balance Criteria:

I. Customers who are maintaining Average Quarterly Balance exceeding Rs 50 lakh in Saving Accounts.

II. Customers who are maintaining Average Quarterly Balance exceeding Rs 100 lakh in Current Accounts.

III. Customers who are maintaining Average Quarterly Balance exceeding Rs 100 lakh in Term Deposit Accounts.

For determining HNIs, the average balances maintained in Saving and Current accounts of the Customer during the preceding two quarters (half year) shall be reckoned.

In case of Term Deposits, Customers who maintained aggregate deposit amount of Rs. 100 lakhs during the preceding two quarters (half year) shall be reckoned.

B) Account Transaction Turnover Criteria:

For determining HNIs, the Individual Customers who had carried out sum of Credit transactions of value exceeding Rs. 500 lakh in Saving Account and / or Rs. 2500 Lakhs in Current/ Cash Credit/ Over Draft accounts during the proceedings two quarters (half year) shall be reckoned.

The classification of customers as HNIs shall be carried out by Central Office based on above criteria at half yearly intervals and will be system driven. The branches should not change the HNI customers determined at system level and there will not be any manual process for classification of HNIs. While on-boarding new customers, branches should not classify any customer as HNI, since the HNIs are determined based on the quarterly average balances maintained/ Transactions Turnover in Accounts as stated above.

Branches shall prepare risk profile of each customer, who has been classified as HNIs by the System and apply enhanced due diligence measures as applicable to High Risk Customers.

3.1.2.10 <u>Accounts of non-face-to-face customers (other than customer onboarding in terms of Section 17)</u>:

The Bank may establish Customer on-boarding in Non-face-to-face mode and such facilitates of the Bank is made available to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes includes use of digital channels such as CKYCR, Digi-Locker, equivalent e-document, etc., and non-digital modes such as

obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. The following EDD measures shall be undertaken for non-face-to-face customer onboarding.

a) The V-CIP process introduced by our Bank shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP.

b) In order to prevent frauds, alternate mobile numbers should not be linked post CDD with such accounts opened through Non-face to face mode, for sharing transaction OTP, transaction updates, etc. Transactions should be permitted only from the mobile number used and registered with the Bank at the time of opening of the account. The request for change of registered mobile number for the accounts opened through Non-face-to-face mode shall be done after undertaking the following measures.

i) The account opened using Non-face-to-face facilities of the Bank are required to be converted to face-to-face mode only after verification of identity of the customer in face-to-face manner or through V-CIP process of the Bank.

ii) In case of requests for change of registered mobile number in such accounts, Branches should permit only after the conduct of customer due diligence by way of e-KYC (biometric/ OTP) authentication facility provided by UIDAI for dealing with requests for change of registered mobile number.

iii) Further, where conduct of e-KYC is not possible, permissions for change in mobile number request should be obtained from Regional Office and Officers working in Regional Office in the rank of Scale-IV and above are authorized to permit such requests.

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

d) Branches should obtain PAN from the customer and the PAN should be verified from the verification facility of the issuing authority (NSDL).

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

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

3.1.2.11 **Guidelines on Walk-in-Customers:** Walk-in Customer means a person who does not have an account-based relationship with the bank, but undertakes transactions with the bank.

a) Transactions carried out by a non-account based customer, that is a walk-in customer, where the amount of transaction, viz. international money transfer operations, issue of travellers' cheques, issuance of demand draft/RTGS/NEFT/EFT, sale of gold coins/silver/platinum/third party products is equal to or exceeds rupees fifty thousand during any one day, whether conducted as a single transaction or several transactions that appear to be connected, should be effected by debit to the customer's account or against cheques only and not against tendering cash and the customer's identity, address and PAN number should be verified.

b) However, if a bank 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 bank should verify the identity and address of the customer and also consider filing a suspicious transaction report (STR) to FIU-IND".

c) Branches have to maintain records in respect of transactions carried out with walk-in customers for a period and in the manner prescribed in Para 10.5 of this policy as in case of any other records as per PML act.

3.1.2.12 Domestic Money Transfer- Relaxations (Walk-in-Customers)

3.1.2.12.1 Payment of amounts transferred from a bank account (Cash Payout Schemes)

Under mobile banking, it is permitted to provide services which facilitate transfer of funds from the accounts of customers for delivery in cash to the recipients not having bank accounts at an ATM or through an agent appointed as Business Correspondent. The ceiling on the value of such transfers has been now raised from Rs.5,000 to Rs.10,000 per transaction subject to the cap of Rs.25,000 per month**.** It has been further decided to permit facilitate such fund transfers through any other authorized payment channels as well. The remitting branches shall obtain full details of the name and address of the beneficiary.

3.1.2.12.2. Payment of amounts to be credited to bank accounts (Cash Pay in Scheme)

A walk-in customer at a bank branch can remit funds up to Rs.50,000to the bank account of a beneficiary through NEFT. Besides, banks are also permitted to allow such customers to transfer funds to a Bank account of a beneficiary through BCs, ATMs, etc. up to a maximum amount of Rs.5,000 per transaction

with a monthly cap of Rs.25,000.Such a walk-in customer needs to provide minimum details like his/her name and complete address to the remitting bank.

3.1.3 WHAT IS VERIFICATION?

Verification of identity is the process of proving whether a person actually is who he claims to be. In the context of KYC, verification is the process of seeking satisfactory evidence of the identity of those with whom the Bank does business. This is done by carrying out checks on the correctness of the information provided by the client. The best available evidence of identity should be obtained, having regard to the circumstances of each client and their country of origin. Some forms of proof of identity are more reliable than others, and in some cases it will be prudent to carry out more than one verification check.

3.1.4 VERIFICATION OF CREDENTIALS/ANTECEDENTS:

Before opening an account, the banker must get true identity of the intending customer verified and his acceptability for establishing business relationship should be ascertained. When the Bank opens an account in the name of a customer, it has to render a number of services, including collection of cheques in the ordinary course of business. It is, therefore, essential that the bank is aware of the credentials of the prospective customer such as his profession, business address, etc. and verification of antecedents of account holder in each and every account is, therefore, essential.

3.1.5 FORMALITIES FOR OPENING OF ACCOUNT:

3.1.5.1. To verify the residential address given by the customer, banks generally ask for copies of passport, driving license, identity card issued by any institution, copy of electricity or telephone bill, copy of any communication issued by Central/State Government authorities showing residential address or any other evidence, in support of the address given in the account opening form.

3.1.5.2. Verification of the residential address provided by the customer is now assuming greater importance. While considering loan products, verification is usually done through a visit. However, this is not possible in all cases of account opening. As such, this may be achieved by mailing a welcome kit containing cheque books, rules book, pamphlets on various schemes of the Bank etc. in the address provided by the customer.

3.1.5.3. The banks also contact customer at the telephone number provided in the account to verify the customer details.

3.1.5.4. While opening accounts of corporate bodies, firms, trusts etc. the banks obtain documentary evidence regarding existence of the entity, powers of authorized persons to operate the account etc.

3.1.5.5. An interview with the prospective customer is recommended while opening an account as the interview would help in knowing the customer and preparing the profile.

3.1.6. Process for Video based Customer Identification (V-CIP):

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

Provided that in case of CDD of a proprietorship firm, branches shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Para 3.1.2.4 of this Policy, apart from undertaking CDD of the proprietor.

ii) Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per Para 3.5.7.

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

Bank / Branches opting to undertake V-CIP, shall adhere to the following minimum standards:

(a) V-CIP Infrastructure:

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

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

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

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

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

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

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

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

(b) V-CIP Procedure:

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

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

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

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

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

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

a. OTP based Aadhaar e-KYC authentication
b. Offline Verification of Aadhaar for identification
c. KYC records downloaded from CKYCR, using the KYC identifier provided by the customer
d. Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digi-locker

It shall ensure to redact or blackout the Aadhaar number in terms of Para 3.1.2.4.

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

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

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

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

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

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

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

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

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

xiv) The procurement of Video CIP application, IT and other infrastructures shall be procured by Central Office and will be integrated with Core banking solution, Internet banking, Mobile banking, Digital banking, USB handset of the Banking Correspondents (BCs) and TAB banking, etc. Further the V-CIP application / app will be also be placed in the Bank's website to facilitate the prospect customers to on-board through Video-CIP.

xv) The entire V-CIP will be handled at a Centralized location including concurrent auditing of the V-CIP process and authorization of the CIFs.

xvi) After the CIFs are authorized and made active, the CIFs will be transferred to the home branch opted / selected by the Customer.

(C) V-CIP Records and Data Management

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

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

3.1.7 Updation/ **Periodical Updation of KYC:**

Bank shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. **However,** Periodic updation of KYC of customer is carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC updation. In terms to amendment to Section 38 of Master Direction on KYC, the following procedure is to be adopted for Re-KYC i.e., Periodic updation of KYC of customers:

1) For Individual Customers:

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

b) Change in address: In case of a change only in the address details of the customer, a self-declaration of the new address shall be obtained from the customer through customer's email -id registered with the bank, customer's mobile number registered with the bank, ATMs, digital channels (such as online banking / internet banking, mobile application of the Bank), letter, courier, etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

Further, branches at their option may obtain a copy of OVD or deemed OVD, **as defined in Section 3(a)(xiv),** or the equivalent e-documents thereof, as defined in Para 3.1.2.4 of this policy, for the purpose of proof of address, declared by the customer at the time of periodic updation.

c) Accounts of customers who were minor at the time of opening account on their becoming major: In case of customers for whom account was opened when they were minor, fresh photographs shall be obtained on their becoming a major and at that time it shall be ensured that CDD documents as per the current CDD standards are available with the branches. Wherever required, branches may carry out fresh KYC of such customers i.e. customers for whom account was opened when they were minor, on their becoming a major.

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

2. Customers other than individuals:

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

b) Change in KYC information: In case of change in KYC information, branches shall undertake the KYC process equivalent to that applicable for on-boarding a new Legal Entity customer.

3. Additional measures: In addition to the above, branches shall ensure that -

a) The KYC documents of the customer as per the current CDD standards are available with them. This is applicable even if there is no change in customer information but the documents available with the Bank are not as per the current CDD standards. Further, in case the validity of the CDD documents available with the branch has expired at the time of periodic updation of KYC, branches shall undertake the KYC process equivalent to that applicable for on -boarding a new customer.

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

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

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

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

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

f) In order to ensure customer convenience, the facility of periodic updation of KYC can be done at any branch of the Bank.

f) Branches should be transparent in dealing with Customers while obtaining KYC records and adverse action against customer should be avoided, unless warranted by specific regulatory requirements.

ii) In view of the press release of RBI dated January 05, 2023 & advisory dated February 16, 2023, the simplified measures as provided by the RBI in terms of Section 38 (a) (i) and (ii) of the MD on KYC i.e., facility of self-declaration by customers through various non-face-to-face channels, in case of no change in KYC information/ change in address only, branches should not insist the Customer for branch visit for periodic updation of KYC. The branches should encourage the simplified measures in non-face-to-face mode for clearing pendency in periodic updation of KYC. Branches are advised to ensure the following timelines for reducing the level of pendency in periodic KYC updation and in sharing of KYC information with CKYCR.

(a) Periodic updation of KYC of all customers having operative accounts that were due for updation as on March 31, 2022 should be completed by June 30, 2023.

(b) KYC records which were due for upload onto CKYCR as on March 31, 2022 should be uploaded within reasonable time, preferably by June 30, 2023.

(c) For the subsequent period (i.e, April 01, 2022 onwards), the periodic KYC updation and uploading of KYC date onto CKYCR should be carried out on an ongoing basis.

3.1.8 Cessation of account for non-submission of PAN or equivalent e-document thereof or Form No.60: In case of existing customers, where the Permanent Account Number or equivalent e-document thereof or Form No.60 are not obtained, by such date as may be notified by the Central Government, then branches shall temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, branches shall give the customer an accessible notice and a reasonable opportunity to be heard.There is relaxation for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise and such like causes. Such accounts shall, however, be subject to enhanced monitoring.

Provided further that if a customer having an existing account-based relationship with a branch gives in writing to the branch that he does not want to submit his Permanent

Account Number or equivalent e-document thereof 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 branch 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.
Further, appropriate relaxation(s) is to be given for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e-document thereof or Form No. 60 owing to injury, illness or infirmity on account of old age or otherwise, and such like causes.

3.2 Customer Due Diligence (CDD) :

The customer due diligence means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

Explanation – The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

a. Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;
b. Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
c. Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.
d. CDD includes as any measures undertaken to collect and verify information and positively establish the identity of a customer. Branches shall obtain information using Aadhaar or 'Officially Valid documents' or the equivalent e-document thereof containing the details of his identity and address including PAN or the equivalent e-document thereof or Form 60from 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. While opening a joint account, CDD procedure including obtaining PAN or the equivalent e-document there of or Form 60 as applicable is to be followed for all the joint account holders.

e. Where branches are unable to comply with the CDD requirements mentioned above, they shall not open accounts, commence business relations or perform transactions. In case of existing business relationship which is not KYC compliant, branches shall ordinarily take step to terminate the existing business relationship after giving due notice.

There are 3 types of CDD that can be used in accordance with the risk category of the customer.

3.2.1 Basic Due Diligence:

Basic Due Diligence means collection and verification of identity proof, address proof and photograph to establish the identity of the customer. This is based on documents and forms the basis of the KYC programme of the bank. A different set of documents can be listed for different type of customers as seen in Para 3.1.2.4. of this Policy.

3.2.2 Simplified Due Diligence:

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

3.2.3 Enhanced Due Diligence (EDD):

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

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

Specific types of relationships where EDD may be required to be applied:

3.2.3.1 Client accounts opened by professional intermediaries:

When the bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified**.** Banks may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the bank, the bank should still look through to the beneficial owners.

Where the branch relies on the 'customer due diligence' (CDD) done by an intermediary, the branch should satisfy itself that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. For the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship, Branches may rely on a third party; subject to the conditions that:-

(a) Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry.

(b) Branch takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;

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

(d) The third party is not based in a country or jurisdiction assessed as high risk; and

(e) The Branch is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable. It should be understood that the ultimate responsibility for knowing the customer lies with the branch.

Further, if the professional intermediaries like Chartered Accountant or lawyer etc. are unable to disclose the true identity of the owner of the account / funds due to any professional obligation of customer confidentiality, branches should not open or hold accounts of professional intermediaries on behalf of a client. Further, because of such obligation on the part of the professional intermediary, branches are unable to know and verify the true identity of the client on whose behalf account is held or beneficial ownership and / or understand the true nature and purpose of transactions, then branches should not open an account, on behalf of a client, by professional intermediary.

3.2.3.2 Accounts of Politically Exposed Persons (PEPs) resident outside India as defined in ParaNo.3.1.2.8

3.2.3.3 Accounts of non-face-to-face customers as defined in Para No.3.1.2.10.

3.2.3.4 **Correspondent Banking**

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable through-accounts, cheques clearing etc.

3.2.3.4.1 Bank should have a policy approved by the Boards, or by a committee headed by the Chairman/CEO/MD to lay down parameters for approving cross-border correspondent banking and other similar relationships. In addition to performing normal CDD measures, such relationships shall be subject to the following conditions:

a. Banks shall gather sufficient information about a respondent bank to understand fully the nature of the respondent bank's business and to determine from publicly available information the reputation of the respondent bank and the quality of supervision, including whether it has been subjected to a ML/TF investigation or regulatory action. Banks shall assess the respondent bank's AML/CFT controls.
b. The information gathered in relation to the nature of business of the respondent bank shall include information on management, major business activities, purpose of opening the account, identity of any third-party entities that will use the correspondent banking services, regulatory/supervisory framework in the respondent bank's home country among other relevant information
c. Prior approval from senior management shall be obtained for establishing new correspondent banking relationships. However, post facto approval of the Board or the Committee empowered for this purpose shall also be taken.
d. Banks shall clearly document and understand the respective AML/CFT responsibilities of institutions involved

(d) In the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has conducted CDD on the customers having direct access to the accounts of the correspondent bank 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 CDD information immediately on request.
(f) Correspondent relationship shall not be entered into or continued with a shell bank.
(g) It shall be ensured that the respondent banks do not permit their accounts to be used by shell banks.
(h) Bank shall be cautious of correspondent banking relationships with institutions located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.
(i) Bank 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.

3.2.3.4.2 Transactions conducted through the correspondent relationships need to be managed taking a risk based approach. Know Your Correspondent procedure should be established to ascertain whether

the correspondent bank or counter party is itself regulated for money laundering prevention and, if so, whether the correspondent is required to verify their customer identity to FATF standards.

3.2.3.4.3 International Division (ID) at C.O will ascertain & ensure that all our banks correspondent and respondent banks have KYC/AML standards in place. ID shall circulate such list of correspondent /respondent banks to all ZOs, ROs, A and B category branches. ID will further review the standards and update the list periodically.

3.2.3.5 **Non-resident Indians (NRIs)/Foreign Nationals**

Indian customers resident overseas and foreign nationals based in India pose a bigger risk from money laundering perspective than ones placed domestically.

3.2.3.6 **Fiduciary Accounts**

Bank may exercise enhanced due diligence at the time of opening fiduciary accounts by intermediaries such as guardians of estates executors, administrators, assignees, receivers etc. for e.g. while opening of the account of an administrator of the estate, it may be necessary to examine the Letter of Administration (Authority) as it would give a picture of the assets of the estate. In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

3.2.3.7.**Due Diligence in Correspondent Banking arrangement with Co-Operative Banks**

Branches have arrangements with co-operative banks wherein the latter open current accounts and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in- customers for facilitating their remittances and payments. Since the 'at par' facility offered by commercial banks to co-operative banks is in the nature of Correspondent banking arrangements, branches should monitor and review such arrangements to assess the risks including credit risk and reputational risk arising therefrom. For this purpose, branches should 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.

3.2.3.8. Customer Due Diligence for transactions in Virtual Currencies (VC):

Reserve Bank has advised to continue to carry out Customer Due Diligence processes in line with regulations governing standards for Know Your Customer (KYC), Anti-Money Laundering (AML), Combating of Financing of Terrorism (CFT) and obligations of regulated entities under Prevention of Money Laundering

Act (PMLA), 2002 in addition to ensuring compliance with relevant provisions under Foreign Exchange Management Act (FEMA) for overseas remittances.

3.3 Correspondent relationship with a "Shell Bank":

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

3.3.1 Branches should refuse to enter into a correspondent relationship with a "shell bank". Shell banks are not permitted to operate in India. Further, before establishing correspondent relationship with any foreign institution, appropriate measures should be taken by the Bank to satisfy themselves that the foreign respondent institution does not permit its accounts to be used by Shell Banks.

3.3.2 Branches should be extremely cautious while continuing relationships with respondent banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing. Branches should ensure that their respondent banks have anti-money laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts. Branches are advised to refer to International Division, Central Office, for clarification /guidance in the matter.

3.3.3 Applicability of KYCAML guidelines to branches and subsidiaries outside India:

3.3.3.1 The guidelines contained in this KYCAML Policy-2024 shall apply to the branches and majority owned subsidiaries located within India. Further these directions shall also apply to branches and majority owned subsidiaries of the Bank which are located abroad, especially in countries which do not or insufficiently apply the FATF Recommendations, to the extent they are not contradictory to the local laws in the Host Country.

provided that:

i. where applicable laws and regulations prohibit implementation of these guidelines, the same shall be brought to the notice of the Reserve Bank of India. RBI may advise further necessary action by the RE including application of additional measures to be taken by the RE to manage the ML/TF risks.
ii. in case there is a variance in KYC/AML standards prescribed by the Reserve Bank of India and the host country regulators, branches/ subsidiaries of REs are required to adopt the more stringent regulation of the two.
iii. branches/ subsidiaries of foreign incorporated banks may adopt the more stringent regulation of the two i.e., standards prescribed by the Reserve Bank of India and their home country regulators.

3.4 Information sought by Banks from Customers, Secrecy Obligation and Sharing of Information:

3.4.1 Seeking personal information/details like number of dependents, the names of sons and daughters, lifestyle, number of foreign visits undertaken during the last three years, details of family members/relatives settled abroad, assets and liabilities, name and date of birth of spouse, wedding date, investments, etc., from customers which are not mandatory and relevant to perceive risk of a prospective customer while complying with KYC/AML requirement during the process of opening an account or during periodic updation. This has led to customer complaints that banks are going overboard in seeking information for KYC compliance and thereby invading into their privacy.

3.4.2 In this connection, attention of branches is drawn that information sought from customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer should be sought separately with his/her consent and after opening the account. It is, therefore, reiterated that 'mandatory' information required for KYC purpose which the customer is obliged to give while opening an account only should be obtained at the time of opening the account/during periodic updation.

3.4.3 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. 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 that is optional.

3.4.4. Further, it is reiterated that branches should 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) collected from the customer is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes without the express permission of the customer.

3.4.5. While considering the requests for data/information from Government and other agencies, branches 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.

The exceptions to the said rule shall be as under:

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

3.5 Guidelines on Aadhaar to be accepted as an "Officially Valid Document" under PML Rules

3.5.1 "Aadhaar number" Every resident shall be entitled to obtain an Aadhaar number by submitting his demographic information and biometric information by undergoing the process of enrolment.

As per Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016); "Aadhaar number" means an identification number issued to an individual based on receipt of the demographic information and biometric information and after verifying the information by the Aadhaar issuing Authority, in such manner as may be specified by regulations, shall issue an Aadhaar number to such individual.

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

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

3.5.4 "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).

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

3.5.6 Aadhaar number can be submitted by a customer where,

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

(b) he decides to submit his Aadhaar number voluntarily to the bank;

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

(d) the proof of possession of Aadhaar number where offline verification cannot be carried out.

(e)Authentication shall be carried out 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, branches 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 branch and such exception handling shall also be a part ofthe concurrent audit as mandated in M D of RBI that Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures. Branches shall ensure to duly record the cases of exception handling in a centralized exception database. The database shall contain the details of grounds of

granting exception, customer details, name of the designated official authorizing 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.
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.

3.5.7 **Accounts opened using OTP based e-KYC, in non-face-to-face mode:** Provided further that branches may provide an option for One Time Pin (OTP) based e-KYC process for on-boarding in non-face to face mode of customers. Accounts opened in terms of this proviso 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. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD for opening a normal account including quoting of PAN / Form 60 is complete.

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

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

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

(vi) 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.

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

(viii)Strict monitoring procedures will include systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

3.6 Guidelines on Unique Customer Identification Code (UCIC)

3.6.1 The increasing complexity and volume of financial transactions necessitate that customers do not have multiple identities within a bank, across the banking system and across the financial system.

3.6.2 Unique identifiers for customers has been introduced within the Bank. In our bank CIF is the Unique Number of customers. The CDD (Customer due diligence) procedure is applied at the UCIC / CIF level itself.

3.6.3 The existing customers having multiple CIFs are being consolidated by the exercise of de-duplication.

3.6.4 While opening of a new account a unique code (only single CIF) for a customer will be allotted. Before allotting a new CIF to a customer, it shall be verified that the customer has not an existing CIF. If a customer has already one CIF the new account(s) shall be tagged with the existing CIF.

3.6.5 The UCIC will also help to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable to have a better approach to risk profiling of customers. It would also smoothen banking operations for the customers.

3.7 <u>CDD Procedure and Sharing KYC information with Central KYC Records Registry (CKYCR) - Roll out of Legal Entity Template & other changes:</u>

(a) Govt. of India has authorized the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI) to act as and perform the function of CKYCR vide Gazette Notification No. S.O. 3183 (E) dated 26th November 2015. "Central KYC Records Registry" means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer. As per the 2015 amendment to PML (Maintenance of Records) Rules, 2005, branches shall capture the KYC information pertaining to all new individuals opened on or after 01 January 2017 for sharing with CKYCR in the manner mentioned in the rules, as per KYC templates finalized by CERSAI and as instructed vide our Circulars in this regard. The KYC records received and stored by the CKYCR could be retrieved online by any reporting entity across the financial sector for the purpose of establishing an account based relationship.

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

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

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

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

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

(e) The 'live run' of the CKYCR started from July 15, 2016 in phased manner beginning with new 'individual accounts'. Accordingly, Our Bank, being a SCB, is are required to invariably upload the KYC data pertaining to all new individual accounts opened on or after January 1, 2017, with CKYCR. The Bank was initially allowed time up-to February 1, 2017, for uploading data in respect of accounts opened during January 2017 with CKYCR in terms of the provisions of the Rules ibid.

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

(g) Once KYC Identifier is generated by CKYCR, it shall ensure that the same is communicated to the individual/Legal Entities as the case may be.

(h) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, The Branches shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to 01.01.2017 & 01.04.2021 respectively **for Individuals & Legal Entities as per clauses (e) and (f),** respectively, at the time of periodic updation as specified **in paragraph 38 of this Master Direction**, **or earlier,** when the updated KYC information is obtained/received from the customer.

(i) Whenever the Bank obtains additional or updated information from any customer as per clause (j) below in this paragraph or Rule 9 (1C) of the PML Rules, the Bank shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs the Bank regarding an update in the KYC record of an existing customer, the Bank shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the Bank in CBS.

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

(k) For the purpose of establishing an account-based relationship, **updation /periodic updation or for verification of identity of a customer, the Bank shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless–**

i. there is a change in the information of the customer as existing in the records of CKYCR**; or**

ii. **the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or**

iii. the validity period of downloaded **documents** has lapsed; **or**

iv. the Bank considers it necessary in order to verify the identity or address **(including current address)** of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the **customer.**

3.8 Compliance of KYC policy: Ensuring compliance with KYC Policy through: (i) Specifying as to who constitute 'Senior Management' for the purpose of KYC compliance. A Senior officer in the rank of General Manager will constitute as 'Senior Management' for the purpose of KYC compliance. (ii) Allocation of responsibility for effective implementation of policies and procedures. The Designated Nodal Officer at all Regional Offices and at all Zonal Offices are designated as Compliance Officers. (iii) Independent evaluation of the compliance functions of Banks' policies and procedures, including legal and regulatory requirements by Compliance Dept, C O. (iv) Concurrent / internal audit system to verify the compliance with KYC/ AML policies and procedures and submit quarterly audit notes and compliance to the Audit Committee. (v) Concurrent / internal audit to also ensure verification of compliance with KYC guidelines in system through system generated reports.

It shall be ensured that decision-making functions of determining compliance with KYC norms are not outsourced.

4 REPORTING REQUIREMENT UNDER FATCA AND CRS

India has signed the Inter-Governmental Agreement with the USA on July 9, 2015 for improving International Tax Compliance and implementing the Foreign Account Tax Compliance Act (FATCA)of the USA. India has also signed a multilateral agreement on June 3, 2015 to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters under the Common Reporting Standards (CRS).

Accordingly, provisions have been made under Income Tax Rules 114F, 114G and 114H. Accounts of persons having tax residency in USA are to be reported under FATCA and persons having tax residency outside India other than USA is reportable under CRS. An account becomes reportable under FATCA/CRS if the account holder/controlling person/s is/are tax resident/s of any country other than India.

Branches are required to compulsorily obtain FATCA / CRS declaration / self-certification from all customers. In the event of non-receipt of self-certification form, the account(s) would be blocked and the transactions by the account holder in such blocked accounts would be allowed once the duly filled self-certification is obtained and due diligence completed. Under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS), Bank is required to adhere to provisions of Income Tax Rules 114F, 114G and 114H and take following steps for complying with the reporting requirements:

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

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

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

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

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

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

(f) Ensure compliance with updated instructions/ rules/ guidance notes/ Press releases/ issued on the subject by Central Board of Direct Taxes (CBDT) from time to time and available on the web site http://www.incometaxindia.gov.in/Pages/default.aspx. Bank may take note of the following(Refer RBI site):

i. updated Guidance Note on FATCA and CRS

ii. apress release on 'Closure of Financial Accounts' under Rule 114H (8).

"CRS" (Common Reporting Standards) 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.

"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.

5. ANTI MONEY LAUNDERING STANDARDS

Money Laundering is the process whereby proceeds of crimes such as drug trafficking, smuggling, terrorism, organized crimes, fraud and many other crimes are converted into legitimate money through a series of financial transactions making it impossible to trace back the origin of funds.

The technological advancements and introduction of New Technologies – Credit Cards /Debit Cards/Smart Cards/ Gift Cards/Mobile Wallet/ Net Banking/Mobile Banking/ RTGS / NEFT /ECS /IMPS etc. have facilitated on line transfer of funds and real time settlement between the Banks across the globe. This has helped money launderers to adopt innovative means and move funds faster across continents making detection and preventive action much more difficult. This calls for a dynamic approach in tracking the crime. The staff members of the Bank must be vigilant in the fight against money laundering and must not allow the bank to be used for money laundering activities. The Bank should not become the party to violation of law. As such, preventing money laundering activities is the duty and responsibility of the bank staff.

Branches should pay special attention to any money laundering and financing of terrorism threats that may arise from new or developing technologies including internet banking that might favor anonymity, and take measures, if needed, to prevent their use in money laundering schemes. As our Bank is engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds, Branches are required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Further, marketing of credit cards is generally done through the services of agents. Branches should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that agents are also subjected to due diligence and KYC measures.

5.1 MONEY LAUNDERING:

As per the Prevention of Money Laundering Act (PMLA) 2002, the offence of Money Laundering is defined as:

Whoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of a crime and projecting the same as a untainted property – shall be guilty of offence of Money Laundering. Money Laundering is the process by which the criminals attempt to hide and disguise the origin and ownership of the proceeds of their criminal activities like drug trafficking, trafficking in women and children, murder, extortion, child pornography etc. 'Proceeds of crime' means any property derived or obtained, either directly or indirectly by any person as a result of criminal activities relating to a scheduled offence or the value of such property. Money Laundering, therefore, besides being a Statutory or Regulatory requirement is also a moral responsibility for all the Bank Employees.

Nomination of Designated Director:

Banks are required to nominate a Director on their Boards as "Designated Director", as per 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.

"Designated Director "means a person designated by the Banks Board to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and includes the Managing Director or a whole-time Director duly authorized by Board of Directors if the reporting entity is a company. In no case, the Principal Officer shall be nominated as the Designated Director. The name, designation and address of the Designated Director are to be communicated to the Director, FIU-IND. In addition, it shall be the duty of every reporting entity, its Designated Director, officers and employees to observe the procedure and manner of furnishing and reporting information on transactions referred to in PML Rule.

Principal Officer:

"Principal Officer" means an officer at the management level nominated by the Bank, responsible for furnishing information as per Rule 8 of the PML rules. Principal Officer is responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law / regulations. The name, designation and address of the Principal Officer are to be communicated to the Director, FIU-IND.

5.2 TERRORIST FINANCING:

Terrorists use similar methods for moving their funds. Some of the terrorist groups also indulge in criminal activities for funding their acts. However, there are two major differences between Money Laundering and Terrorist Financing.

4.2.1 Whereas in the case of Money Laundering, the source of money is always through criminal activities while Terrorist Financing can be from legitimately obtained income.

4.2.2 It is difficult to identify terrorist funding transactions as more often terrorist activities require small amounts.

5.3 WIRE TRANSFERS: "

5.3.1 Wire transfer" related definitions:

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

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

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

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

e. Cross-border wire transfer: Cross-border wire transfer refers to any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.

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

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

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

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

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

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

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

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

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

5.3.2 Wire Transfer:

Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analyzing suspicious or unusual activity and disseminating it as necessary. The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits. Accordingly, branches must ensure that all wire transfers are accompanied by the following information:

5.3.3 Information requirements for wire transfers as per the latest Master Direction's of RBI on KYC:

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

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

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

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

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

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

v. In case of domestic wire transfers below rupees fifty thousand where the originator is not an account holder of the ordering Bank and where the information accompanying the wire transfer can be made available to the beneficiary Bank and appropriate authorities by other means, it is sufficient for the ordering Bank to include a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. The ordering Bank shall make the information available within three working/business days of receiving the request from the intermediary Bank, beneficiary Bank, or from appropriate competent authorities.

i Information accompanying all domestic wire transfers of Rs.50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name; address and account number etc.,

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

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

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

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

a. Any transfer that flows from a transaction carried out using a credit card / debit card / Prepaid Payment Instrument (PPI), including through a token or any other similar reference string

associated with the card / PPI, for the purchase of goods or services, so long as the credit or debit card number or PPI id or reference number accompanies all transfers flowing from the transaction. However, when a credit or debit card or PPI is used as a payment system to effect a person-to-person wire transfer, the wire transfer instructions shall apply to such transactions and the necessary information should be included in the message.

b. Financial institution-to-financial institution transfers and settlements, where both the originator person and the beneficiary person are regulated financial institutions acting on their own behalf. It is, however, clarified that nothing within these instructions will impact the obligation of an RE to comply with applicable reporting requirements under PML Act, 2002, and the Rules made thereunder, or any other statutory requirement in force.

5.3.4 Responsibilities of ordering Bank, intermediary Bank and beneficiary Bank, effecting wire transfer, are as under:

i. Ordering Bank:

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

ii. Intermediary Bank:

a. The Bank processing an intermediary element of a chain of wire transfers shall ensure that all originator and beneficiary information accompanying a wire transfer is retained with the transfer.
b. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary Bank shall keep a record, for at least five years, of all the information received from the ordering financial institution or another intermediary Bank.
c. Intermediary Bank shall take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures should be consistent with straight-through processing.

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

iii. Beneficiary Bank:

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

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

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

5.3.5 Other Obligations:

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

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

a. there is unhindered flow of complete wire transfer information, as mandated under these directions, from and through the unregulated entities involved;
b. the agreement / arrangement, if any, with such unregulated entities by the Bank clearly stipulates the obligations under wire transfer instructions; and

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

ii. Banks' responsibility while undertaking cross-border wire transfer with respect to name screening (such that they do not process cross-border transactions of designated persons and entities):
As per RBI Master Directions, Banks are prohibited from conducting transactions with designated persons and entities and accordingly, in addition to compliance with Chapter IX of the Master Direction, Bank shall ensure that they do not process cross-border transactions of designated persons and entities.

iii. Banks' responsibility to fulfil record management requirements

Complete originator and beneficiary information relating to wire transfers shall be preserved by the Bank, for all the wire transfer transactions undertaken by the Bank, strictly in accordance with the Section 46 of the Master Direction of RBI.

5.4 CHECK LIST FOR PREVENTING MONEY-LAUNDERING ACTIVITIES

The illustrative checklist for preventing money-laundering activities is asunder:

5.4.1 A customer maintains multiple accounts, transfer money among the accounts and uses one account as a master account from which wire/funds transfer originates or into which wire/funds transfer are received (a customer deposits funds in several accounts, usually in amounts below a specified threshold and the funds are then consolidated into one master account and wired outside the country.)

5.4.2 A customer regularly depositing or withdrawing large amounts by a wire transfer to, from, or through countries that are known sources of narcotics or where Bank secrecy laws facilitate laundering of money.

5.4.3 A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer's business or history.

5.4.4 A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.

5.4.5 A customer experiences increased wire activity when previously there has been no regular wire activity.

5.4.6 Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.

5.4.7 A business customer uses or evidences of sudden increase in wired transfer to send and receive large amounts of money, internationally and/or domestically and such transfers are not consistent with the customer's history.

5.4.8 Deposits of currency or monetary instruments into the account of a domestic trade or business, which in turn are quickly wire transferred abroad or moved among other accounts for no particular business purpose.

5.4.9 Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.

5.4.10 Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.

5.4.11 Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency.

5.4.12 Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.

5.4.13 Periodic wire transfers from a person's account/s to Bank haven countries.

5.4.14 A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.

5.4.15 A customer or a non-customer receives incoming or makes outgoing wire transfers involving currency amounts just below a specified threshold or that involve numerous Bank or travellers cheques.

5.4.16 A customer or a non-customer receives incoming wire transfers from the Bank to 'Pay upon proper identification' or to convert the funds to bankers' cheques and mail them to the customer or non-customer, when the amount is very large (say over Rs.10lakhs).

- The amount is just under a specified threshold (Rs.10lacs)
- The funds come from a foreign country or
- Such transactions occur repeatedly.

5.4.17 A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Banker's cheques (just under a specified threshold)

5.4.18 A non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit.

5.5 Money Laundering and Terrorist Financing (ML/ TF) Risk Assessment:

a) As per Section (5A) of Chapter II of the MD on KYC 2016, the Bank is required to 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 our Bank. Further, the periodicity of risk assessment exercise shall be determined by the Board, or any committee of the Board of the Bank to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

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

d) Bank shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on their own or through national risk assessment) and should have Board approved policies, controls and procedures in this regard. Bank shall implement a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, REs shall monitor the implementation of the controls and enhance them if necessary.

5.6: Introduction of New technologies/ products:

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

(a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services and technologies; and

(b) Adoption of risk-based approach to manage and the risks through appropriate EDD measures and transaction monitoring, etc., to manage and mitigate the risks.

6. MONITORING OF TRANSACTIONS – ON-GOING DUE DILIGENCE :

On-going Due Diligence" means regular monitoring of transactions in accounts to ensure that **those** are consistent with Bank's knowledge about the customers, customers' business and risk profile, the source of funds / wealth.

To obviate the scope for frauds and prevent Money Laundering, regular monitoring and supervision of accounts is essential. By understanding the normal and reasonable activity of the customers, coupled with controlling the accounts effectively, risk can be reduced.

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

Monitoring customer activity and transactions throughout the relationship helps the Banks to know their customers, assess risk and provides greater assurance that the Bank is not being used for the purposes of financial crime. However, the extent of monitoring shall be aligned with the risk category of the customer.

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

(a) Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account.
(b) Special attention should be paid to the large and complex transactions including RTGS transactions and all unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or lawful purpose.
(c) Transaction which exceeds the threshold prescribed for specific categories of accounts.
(d) Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

High risk accounts have to be subjected to more intensified monitoring.

A system of periodic review of risk categorization of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be undertaken.

"Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes-
(i) Opening of an account;
(ii) 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;
(iii) The use of a safety deposit box or any other form of safe deposit;
(iv) Entering into any fiduciary relationship;
(v) Any payment made or received in whole or in part of any contractual or other legal obligation;
(vi)Establishing or creating a legal person or legal arrangement.

6.1 MONITORING OF CASH TRANSACTIONS: Permanent account number (PAN) of customers shall be obtained and verified from the verification facility of the issuing authority while

undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time.

6.1.1. To effectively track the cash transactions of Rs. 10 lacs and above (or its equivalent in foreign currency) branches should monitor the details of individual cash deposits and withdrawals of Rs.10 lacs and above on following parameters:

Date of Transaction
Type of account/account no.
Title of account/Name of account holder
Date of opening the account
Amount of Deposit/withdrawal
Identity of the person undertaking the transaction
Name of the beneficiary of the cheque (in case of withdrawal)
Destination of the funds and the form of instruction/authority

6.1.2**.** Wherever the depositor/borrower is depositing/withdrawing cash forRs.10 lakhs and above, which is inconsistent with the normal and expected activity of the customer, the information gathered/revealed from the client as to the source/purpose shall be recorded and reported to Regional Office.

6.1.3 Regional Office on receipt of these statements from the Branches should immediately scrutinize the details thereof. In case any of the transactions prima-facie appears to be dubious or gives rise to suspicion, such transactions should be looked into by deputing officials from Regional Office. If any of the transaction is found to be of suspicious nature, it should be immediately informed to Zonal Manager/Field General Manager, Audit & Inspection Department, AML Cell, Compliance Department, and Central Office.

6.1.4 Under the Prevention of Money Laundering Act' 2002 (PMLA) and Rules notified there under impose an obligation on banking companies, financial institutions and intermediaries of the securities market to verify identity of clients, maintain records and furnish information of details of the following cash transactions in "Cash Transaction Report (CTR)" to FIU-IND on monthly basis on or before 15th of succeeding month.

(a) All cash transactions of the value of more than Rupees ten lakhs or its equivalent in foreign currency.

(b) All series of cash transactions integrally connected to each other, which have been valued below Rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of Rupees ten lakhs or its equivalent in foreign currency.

DIT will generate CTR reports and provide the same in XML formation monthly basis, which are being filed online on FINnet site of FIUIND.

6.2 Monitoring of other transactions

6.2.1 Branches should closely monitor the newly opened accounts in the initial 3 to 6 months of their opening and track the transactions not in line with the profile of the customer.

6.2.2 Branches shall closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies.
Explanation: Cases where a large number of cheque books are sought by the company and / or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.

6.2.3 There have been increased instances of fictitious offers, where fraudsters are using RBI's corporate logo/name or any other reputed company in their e-mail messages to convince the victims of the authenticity of the purported messages conveying lottery/prize winning. The fraudsters persuade victims into making initial payment in a specified bank account towards the charges for clearance of the prize money. Branches should handle the quires in this respect and sensitize the customers.

6.2.4 Wherever the request is received for change in Mobile number, loss of SIM Card, complaints of sudden inactivation or failure of mobile connection, branch should subjectsuch accounts through enhanced monitoring and multiple checks, including calling on such mobile number/land line number seeking confirmation through other modes like e-mail etc.

6.2.5 Any such incident should immediately be reported to Regional Office/Zonal Office and AML Cell, CO.

6.3 In order to strengthen the ongoing due diligence of customers and monitoring of transactions, the Bank should explore the possibility of adoption of appropriate innovative technologies such as Artificial Intelligence and Machine Learning (AI & ML) to support system driven effective ongoing monitoring.

7. Combating Financing of Terrorism:

7.1 Requirements/ obligation under International Agreements & Communication from International Agencies

7.1.1 Branches shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, they do not have any account in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC).

The details of the two lists are as under:

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

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

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

7.1.3 Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs (MHA) as required under UAPA notification dated February 2, 2021 (Annex IV of this KYCAML Policy).

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

7.1.5 Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005): Please refer Annexure-V.

a. **Bank should ensure meticulous compliance with the "Procedure for Implementation of** Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated 1st September, 2023**,** by the Ministry of Finance, Government of India (Annex V of this KYCAML Policy of the Bank).

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

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

d. In case of match in the above cases, bank shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005.

   A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. Bank shall file an STR with FIUIND covering all transactions in the accounts, covered above, carried through or attempted. It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the Central nodal Officer (CNO).

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

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

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

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

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

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

i) Bank shall undertake countermeasures when called upon to do so by any international or intergovernmental organisation of which India is a member and accepted by the Central Government.

7.1.8 Jurisdictions that do not or insufficiently apply the FATF Recommendations:

(a) FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. Bank shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

(b) Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.
Explanation: The processes referred to in (a) & (b) above do not preclude the Bank from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

(c) The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.

7.1.10 Bank is required to procure, implement the latest technological innovations and tools for effective implementation of name screening & transaction screening to meet the sanctions requirements.

7.1.11 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. These lists are integrated with CBS for 100% match and for more than 90% match available at Bank's ftp server and the path - ftp://centftp.cbi.co.in/public/aml.

Branches are advised that before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the list. Further, branches should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to Compliance Officer at ROs / Principal Officer for onward submission to

FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated February 02, 2021 and amended vide corrigendum dated March 15, 2023.

7.1.12 As per the instructions from the Ministry of Home Affairs (MHA), any request for delisting received by any Banks is to be forwarded electronically to Joint Secretary (CTCR), MHA for consideration. Individuals, groups, undertakings or entities seeking to be removed from the Security Council's ISIL (Da'esh) and Al-Qaida Sanctions List can submit their request for delisting to an independent and impartial Ombudsperson who has been appointed by the United Nations Secretary-General. More details are available at the following URL: https://www.un.org/securitycouncil/ombudsperson/application.

7.2 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. Banks are, therefore, advised to develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.

7.3 As per the communication received from the Financial Action Task Force (FATF), the strategic AML / CFT deficient jurisdiction are divided into 3 groups as under:

7.3.1 Jurisdictions subject to FATF call on its members and other jurisdictions to apply counter measures to protect the international financial system from the ongoing and substantial money laundering and terrorist financing (ML/FT) risks emanating from the jurisdiction: Iran

7.3.2 Jurisdictions with strategic AML/CFT deficiencies that have not committed to an action plan developed with the FATF to address key deficiencies as of February 2010. The FATF calls on its members to consider the risks arising from the deficiencies associated with each jurisdiction viz; Angola, Democratic People's Republic of Korea (DPRK), Ecuador and Ethiopia.

7.3.3 Jurisdictions previously publicly identified by the FATF as having strategic AML/CFT deficiencies, which remain to be addressed as of February 2010: Pakistan, Turkmenistan and Sao Tome and Principe.
Further, special attention should be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF statements.

Further, there should be ongoing monitoring. The background and purpose of transactions with persons (including legal and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations (as mentioned above), should be examined and if it appears that such transactions have no apparent economic or visible lawful purpose, the background and purpose of the transactions should be examined, findings to be recorded and all documents and the written findings should be retained and made available to Reserve Bank of India /other authorities, on request.

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

The procedure laid down in the UAPA Order dated 2nd February, 2021 (amended vide corrigendum dated March 15, 2023) as provided in Annex IV of this KYC AML Policy, shall be meticulous followed and compliance of the Order issued by the Ministry of Home Affairs (MHA), Government of India shall be ensured.

Further, The procedure for implementation of Section 12A of " The weapons of Mass Destruction and their delivery Systems (Prohibition of unlawful activities) Act, 2005 as per Ministry of Finance, Govt. of India order dated 30th January, 2023 as provided in Annex-V of this KYC AML Policy, shall be meticulous followed and compliance of the Order issued by the Ministry of Finance (MoF), Government of India shall be ensured.

7.4.1 Freezing of accounts as per Law Enforcement Agencies & Regulatory authorities.

Central Bureau of Investigation (CBI), Central Board of Direct Taxes (CBDT), Enforcement Directorates (EDs), Directorate of Revenue Intelligence (DRI) and Central Economic Intelligence Bureau (CEIB) are the major Law enforcement agencies in India. The Reserve Bank of India (RBI), Financial Intelligence Unit- India (FIU-IND), Securities and Exchange Board of India (SEBI), Insurance Development & Regulatory Authority (IRDA) and PFRDA etc., are regulatory authorities. Orders received from any of the Law Enforcement Agencies & Regulatory authorities against any of the Bank's Customer should be frozen or amount specified in the order should be kept on hold immediate on receipt of such order.

7.4.2 Freezing of Accounts of Companies stuck- off by ROC

Section 248 of Companies Act 2013 empowers Registrar to remove the name of Companies from Register of Companies. Branches should ensure to Freeze the accounts of such struck-off Companies.

7.5 What is 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 reasonable ground of suspicion that it may involve the proceeds of a crime 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;
d. gives rise to reasonable ground of suspicion that it may involve financing of activities of terrorism.
e. Further, when the branch is unable to verify the identity and / or obtain documents required or non-reliability of the data /information furnished to the Bank and is unable to apply appropriate customer due diligence measures and therefore believes that it would no longer be satisfied that it knows the true identity of the customer, besides taking a decision whether to continue the business relationship, should also file an STR with FIU-IND.
f. Where Bank is suspicious of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the

CDD process, and instead file an STR**.** Branches need to have regard to the indicators of suspicion, to determine whether or not a transaction is suspicious. An Indicative list of suspicious activities is given hereunder:

7.5.1 **AN INDICATIVE LIST OF SUSPICIOUS ACTIVITIES**

Transactions Involving Large Amount of Cash

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

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

7.5.1.3Frequent withdrawal of large amounts by means of cheques, including traveller's cheques;

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

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

7.5.1.6 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, bills of exchange etc;

7.5.1.7 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.

Transactions that do not make Economic Sense

7.5.1.8 A Customer having a large number of accounts with the same bank, with frequent transfers between different accounts.

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

7.5.2. Activities non-consistent with the customer's declared business/profile

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

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

7.5.2.3 Unusual applications for DD/TT/PO against cash.

7.5.2.4 Accounts with large volume of credits through DD/TT/PO whereas the nature of business does not justify such credits.

7.5.2.5 A single substantial cash deposit composed of many high denomination notes.

7.5.2.6 Frequent exchanges of small denomination notes for large denomination notes or vice versa.

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

7.5.3. Attempts to avoid reporting/record-keeping requirements.

7.5.3.1 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.

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

7.5.3.3 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.

7.5.4. Unusual activities

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

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

7.5.4.3 An account that has frequent deposits of large amounts of currency bearing the labels of other banks.

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

7.5.5.Customer who provides insufficient or suspicious information

7.5.5.1 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. In this case account need not be opened.

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

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

7.5.6.Certain suspicious funds transfer activities

7.5.6.1 Sending or receiving frequent or large volumes of cross border remittances.

7.5.6.2 Receiving large TT/DD/NEFT/RTGS/EFT remittances from various centers and remitting the consolidated amount to a different account/center on the same day leaving minimum balance in the account.

7.5.7 Operation of bank accounts & Money Mules:

7.5.7.1 "Money mules" can be used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal **access to** deposit accounts by recruiting third parties to act as "money mules." **Banks shall undertake diligence measures and meticulous monitoring to identify accounts which are operated as Money Mules and take appropriate action, including reporting of suspicious transactions to FIU-IND. Further, if** it is established that an account opened and operated is that of a Money Mule, **but no STR was filed by the concerned bank**, it shall **then** be deemed that the bank has not complied with these directions.

7.5.7.2 In a money mule transaction, an individual with a bank account is recruited to receive 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. 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 enforcement agencies to locate the account holder. Sometimes transactions related to money laundering or terrorist financing are carried out through **Money Mules.**

7.5.7.3 The operations of such mule accounts can be minimized if branches strictly follow the guidelines of KYC/AML/CFT/Obligation of banks under PMLA, 2002 issued from time to time and to those relating to periodical updation of customer identification data after the account is opened and also to monitoring of transactions in order to protect themselves and their customers from misuse by such fraudsters. If it is established that an account opened and operated is that of a Money Mule, it shall be deemed that the branch has not complied with these directions.

7.5.7.4 Identification and monitoring of Money Mule Accounts: Considering the advisory/ notification issued by RBI, it is proposed to incorporate the criteria for flagging of accounts as "Suspected Money Mule" and monitoring of transactions in these accounts closely for identification of suspicious transactions: The criteria for identification of "Suspected Money Mule" account is as under.

1. All Small Accounts opened under product codes:
   1029/3401-Cent Vikas Khata (FI/BC)
   1029/1401-Cent Vikas Khata
   1029/1501-Cent Vaibhav (FI/BC)
   1501/3401-Cent Bachat
   1501/1401-Cent Bachat
   1150/1401-SB-Cent Muskan
   And/or all SB and CD accounts (ALL SB/CD product Codes) in the name of Individuals, which are not operated for one Year or more and.
2. Accounts, fulfilling above criteria having outstanding balance upto Rs/- 2000 for one year or more continuously and,
3. Received multiple credits (10 and above) within a period of 7 calendar days, in such accounts and the amount of each transaction is less than Rs/ 2000/- and,

4. Finally the amount deposited is withdrawn from the account immediately within 2 days (either in cash, transfer, single or multiple).

The accounts filtered after applying above criteria i.e. accounts fulfilling above mentioned criteria from I to IV shall be flagged as "SUSPECTED MONEY MULE" accounts in CBS and transactions in these accounts are to be monitored closely for identification of Suspicious transactions.

7.5.7.5 Customer Due Diligence and transaction monitoring.

Accounts identified as "Suspected Money Mule" will be subjected to enhanced Due Diligence within a period of 30 days of account identified as "Suspected Money Mule" account in CBS. Following measure will be carried out:

1. AML alerts generated by AMLOCK system in these accounts will be monitored at CO level for filing STR's.
2. Branches to verify the status of the company from MCA site, at the time of at the time of customer on-boarding, to prevent on boarding of Shell and Struck Off Companies.
3. Enhanced monitoring of transactions in accounts of Fintech players.
4. Enhanced monitoring of transactions done through digital delivery channels by DP & TB Department.

7.5.8. Certain bank employees arousing suspicion

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

7.5.8.2 An employee who is reluctant to take a vacation.

7.5.8.3An employee who is associated with mysterious disappearance or unexplained shortages of significant amounts of bank funds.

7.5.8.4 Negligence of employees/willful blindness is reported repeatedly.

7.5.9 SOME EXAMPLES OF SUSPICIOUS ACTIVITIES/TRANSACTIONSTO BE MONITORED BY THE OPERATING STAFF:

7.5.9.1 Large Cash Transactions.

7.5.9.2 Multiple accounts under the same name.

7.5.9.3 Frequently converting large amounts of currency from small to large denomination notes.

7.5.9.4 Placing funds in Term Deposits and using them as security for more loans.

7.5.9.5 Large deposits immediately followed by wire transfers.

7.5.9.6 Sudden surge in activity level.

7.5.9.7 Same funds being moved repeatedly among several accounts.

7.5.9.8 Multiple deposits of money orders, Banker's cheques, drafts of third parties.

7.5.9.9 Transactions inconsistent with the purpose of the account.

7.5.9.10 Maintaining a low or overdrawn balance with high activity.

7.6.1 Issue/Payment of Demand Draft/ TT etc., Sale of Gold Coins:

(a). In order to curb the misuse of banking channels for violation of fiscal laws and evasion of taxes, Demand Drafts, Telegraphic transfers, Sale of Gold Coin and Third Party Products for Rs. 50,000/- and above should be issued only by debit to the customer's account or against cheque or other instruments tendered by the purchaser and not against cash payment.

(b). Similarly, payments against Demand Drafts, Telegraphic Transfer, Sale of Gold Coin and Third Party Products for Rs. 50,000/- and above should be made through banking channels only and not in cash.

(c). All the transactions carried out by a single customers during a day should be aggregated to arrive the ceiling of Rs.50000/-.Further 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.

(d). This 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.

(e). Further, the name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheques, etc., by the issuing branch. These instructions takes effect for such instruments issued on or after September 15, 2018.

7.6.2 Quoting of PAN:

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

7.6.3 Sale of Third Party Products:

Branches 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 as required under Section 3 of this Policy

(b) Transaction details of sale of third party products and related records shall be maintained as prescribed in Section 10.5 "PRESERVATION OF RECORDS" of this Policy.

(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.
- 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.

8. REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT - INDIA (FIU- INDIA) UNDER PMLACT 2002

a. Bank shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.
Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the Bank for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

b. The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website http://fiuindia.gov.in. shall be made use of by the bank which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data.

c. While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. Bank shall not put any restriction on operations in the accounts where an STR has been filed and 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.

d. While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. Bank shall not put any restriction on operations in the accounts merely on the basis of the STR filed. Where an STR has been filed, Bank and it officials shall keep the fact of furnishing of STR strictly confidential. Further, it should be ensured that there is no tipping off to the customer at any level.

e. Bank, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director is confidential. However, such confidentiality requirement shall not inhibit sharing of information under Section 4(b) of this Master Direction of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

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

8.1 The prevention of Money Laundering Act, 2002 (PMLA) forms the core legal framework put in place by India to combat Money Laundering and Terrorism financing. In terms of the rules notified under PMLA Act 2002, certain obligations have been cast on the Banks with regard to reporting certain transactions. The same are detailed here under:

(a) Cash transaction Report (CTR).
(b) Non-Profit Organization Report (NTR)
(c) Counterfeit Currency Report (CCR) and
(d) Suspicious Transaction Report (STR)
(e) Cross Border Wire Transfer Report (CBWT)

8.1.1 Cash Transaction Report (CTR):

As per PMLA rules, Bank is required to submit details of

a) All cash transactions of the value of more than Rupees Ten lakhs or its equivalent in Foreign Currency.
b) All series of transactions integrally connected to each other which have been valued below Rs. Ten lakhs or its equivalent in Foreign Currency, where series of such transactions have taken place within a month and the monthly aggregate exceeds an amount of Rupees Ten lakhs or its equivalent in foreign currency.
c) The report is to be filed in the format prescribed by FIU-IND.
d) CTR should contain only the transactions carried out by our Bank on behalf of the customers/clients excluding the transactions between the internal accounts of the Bank.
e) While filing CTR, individual transactions below Rs. 50,000/- need not be furnished in transaction file.
f) CTR for every month should be submitted to FIU-IND, by the15th of the succeeding month.

8.1.2 **Non-Profit Organization Transaction Report (NTR):**

"Non-profit organizations" (NPO) means any entity or organization, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.

Explanation for "Non-profit organizations" (NPO):

DARPAN ID is mandatory for creation of new CIFs for all NPO Customers types and to be fed in all existing NPO Customers, who are having accounts in our Bank. The Structure of NPO DARPAN ID : 2 digit alpha (state)/ 4 digit number (year) /unique 7 digit number.

Examples: DL/2024/0001234, here DL represents state, 2024 represents year of registration& 0001234 represents ID assigned to the NPO.

As per PMLA Rules-2005, it is mandatory for all Non-profit Organizations (NPOs) Viz., Trusts, Societies and Section-8 Companies, who have established Trust/ Society/ Company for Charity or Religious or Non-profit Making activities such as "Relief to the poor, education, medical relief, preservation of environment (including watersheds, forests and wildlife) and preservation of monuments or places or objects of artistic or historic interest, and the advancement of any other object of general public utility, are required to mandatorily Register themselves in the DARPAN Portal of NITI Aayog and are required to submit DARPAN ID to the Bank.

Henceforth, any new relationship with an NPO shall be initiated by Branches only after obtaining (post-submission) DARPAN ID from the NPO. For clarity sake, the CIF & Account of NPO should be opened in CBS, only DARPAN ID is submitted by the Trust/ Society/ Section-8 (Non Profit Making) Company.

In case of NPOs, Bank is required to submit the following details of NPOs to Regulators such as RBI/ FIU-IND as under:

(a) All Credit transactions involving receipts of value more than Rs.10 lakhs or its equivalent in foreign currency by clients who are non-profit organizations.

(b) NTRs must contain details of legal persons as per definition under Rule 2(1) (ca) of the Money Laundering (Maintenance of Records) Rules, 2005. The definition of NPO as provided in the above paragraph.

(c) Transactions of an account should be given in report along with details of the legal entity, individuals, account and transaction on lines similar to those for CTRs.

(d) The report is to be filed in the format prescribed by FIU-IND

(e) NTR for every month should be submitted to FIU-IND, by the 15th of the succeeding month.

8.1.3 **Counterfeit Currency Report (CCR):**

All Cash transactions where forged or counterfeit currency notes or bank notes has been used as genuine or where any forgery of valuable security or a document has taken place facilitating the transactions, is to be reported by the 15th day of the succeeding month to FIU-IND. Each entry in the CCR should give complete particulars of the account in which such currency is/was deposited. Whereas the counterfeit currency or forged notes transactions have to be reported as per the format prescribed by FIUIND (Counterfeit Currency Report – CCR), transactions involving forgery of valuable security or document may be reported in plain text form.

8.1.4 **Suspicious Transaction Report (STR):**

8.1.4.1 All suspicious transactions whether or not made in cash, should be reported within 7 days of arriving at a conclusion that any transaction is of suspicious nature. It

should be ensured that there is no undue delay in arriving at a conclusion whether or not a transaction is of suspicious nature and that the principal officer should record his reasons for treating any transaction or a series of transactions as suspicious nature.

8.1.4.2 Utmost care has to be exercised while drafting the Grounds of Suspicion (GOS), as GOS is the most important part of STR. The GOS should clearly express '**Why'** the transaction or activity is unusual, unjustified, does not have economic rationale or bonafides, keeping in mind the Banking Business and services rendered by the Bank. Specific reference needs to be drawn to the customer's profile, apparent financial standing, past activity in the account, business profile, general pattern etc. An indicative list of Grounds of Suspicion is enclosed as Annexure III.

8.1.5 **Cross Border Wire Transfer Reports (CBWT)**

(a)Every Branch is required to maintain the record of all transactions including the record of all cross border wire transfers of more than Rs. 5 lakhs or its equivalent in foreign currency, where either the origin or destination of the fund is in India.

(b)Cross-border Wire Transfer Report (CBWT) for every month should be furnished to Director, FIU-IND by 15th of the succeeding month.

(c)The information is to be furnished electronically in the FIN-Net module developed by FIU-IND.

8.1.6 **Delay in Reporting to FIU-IND**

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 a misrepresented transaction beyond the time limit as specified in this rule shall constitute a separate violation.

8.1.7 **Attempted Money Laundering Transactions:**

In case a transaction is abandoned / aborted by customers, on being asked to produce details / or to provide information, the Bank should report all attempted transactions, even if not completed by customers irrespective of the amount of transaction, in STR.

8.1.8 **Need to file Repeat STR:**

In cases, where STR has been filed in a particular account and fresh alerts are observed in the same account, the following factors have to be considered by the Bank, to judge and to take a decision for filing a repeat STR.

8.1.8.1 Has any additional ground of suspicion which has not been reported earlier, been noted observed?

8.1.8.2Is the alert value / volume/ frequency is substantially high as compared to the earlier?

8.1.9 **How to deal with the reported accounts?**

The accounts reported in STR should be classified as high risk and should be subjected to enhanced monitoring. If significant activity is observed in these accounts, a repeat STR may be sent. Further, the competent authority should take a decision regarding closure of such an account / accounts where STR is repeatedly reported. However, such customers should not be tipped off.

8.1.10 **Tipping off the customer:**

There are no restrictions as such on the Banks to discontinue operations in an account, which was reported in STR, to FIU-IND. In case, any restrictions have been placed in any account, it should be ensured by the branches that there is no tipping off the customer at any level. Tipping off would mean informing/communicating to the customer that his/her/their account has been or would be reported for suspicious activity to the Regulators/FIU-IND. However, seeking information about a particular transaction as part of the due diligence, should not tantamount to tipping off. Mentioned hereunder are some suggestions to avoid tipping off, which should be complied with by the field functionaries.

8.1.10.1 Due diligence should be preferably by way of pretext sales calls.

8.1.10.2 No statement should be made, which cautions or warns the customer.

8.1.10.3 AML triggers/rules/reporting thresholds and internal monitoring processes should not be discussed with the customers.

8.1.10.4 The conclusion that has been arrived at after making the necessary enquiries should not be revealed to the customer.

8.1.10.5 No disclosure should be made to the customers that his/her accounts are under monitoring for suspicious activities or that STR has been filed/is being filed against him/her.

8.1.11 **Procedure of STR Alerts scrutiny:**

8.1.11.1 The STR alerts, based on scenarios, are generated through AML software (AML system). A team of front line officers at AML-KYC Cell are screening the generated STR alerts. After first level checking by a Senior Manager and second level checking by Chief Manager, the suspicious alert shall be put up before the

Principal Officer for his approval to file an STR to FIU-IND by AML Cell, CO, uploaded electronically on its FIN net site.

Indicative guidelines given to Front line Officers (MLRO) for monitoring of alerts:-

i. There is a break in threshold transaction of cash deposits in amounts ranging between INR 9,90,000/- to INR 9,99,999.99) in multiple accounts (under same CIF) of the customer and Deposit of cash in the account in amounts ranging between INR 40,000/- to INR 49,999/-

ii. Money is credited from different locations into an account and immediately withdrawn.

iii. Money credited / transaction observed in the account is inconsistent with the profile of the customer.

iv. There is a continuous flow of credit in cash and money is immediately transferred to another account, either in our bank or some other Bank of the same party or of related party.

v. There is cyclic movement of funds between different parties

vi. There is high activity of credit or debit in newly opened accounts.

vii. There is sudden high activity or huge cash deposits in an in-operative accounts.

viii. The account is closed within six months or activity in the account slows down thereafter.

ix. MLRO should see history of generated alerts in the account if there are continuous generation of alerts in the same or different scenarios, the account should be carefully examined.

The said guidelines are only indicative and not exhaustive and MLRO will scrutinize the alerts and take decision on case to case basis.

If the transactions / activity in the account where alert is generated is apparently commensurate with the profile of the customer and /or on further investigation, the transactions / activity appears to be genuine and no suspicion is observed, MLRO will close the alerts.

The first level Officer (Senior Manager), second level Officer (Chief Manager) and Principal Officer shall randomly check the alerts closed by MLRO to assess the quality of closure and in case any suspicious activity is observed in the closed alerts on random checking , the same shall be re-examined and STR be filed with FIU – INDIA.

8.1.11.2 In case of exigencies the STR alerts will be decentralized to all the Regions for screening.

8.1.11.3 Regional Offices will designate officers as Money Laundering Reporting Officer (MLRO) for scrutiny of STR alerts. The Chief Manager, looking after the functions of Operations Department or Second officer in command at all the Regions is designated as 'Compliance Officer' who is responsible for implementation of instructions issued on KYC-AML. He shall also act as first level checker for the screened STR alerts/referred probable STR cases by the designated MLROs at ROs and forward the report to KYC-AML Cell, Central Office.

8.1.11.4The 'Compliance Officer' at ROs will monitor the effective and authentic screening of STR alerts and remarks put for closure of STR alerts.

8.1.11.5 During course of screening of STR alerts, information sought for further investigation from branches should be furnished/ replied within a stipulated time of THREE days from receipt of the query. If no response is received, the matter will be escalated to higher authorities after seven days

8.1.12Measures for improvement of screening of STR alerts

8.1.12.1 The following procedure will be adopted for fastest scrutiny and closure:

a) The STR alerts screening may be partially decentralized at RO level.
b) By adopting the above method the manpower and man hours will be saved which can be utilized for monitoring and follow up.

9. RISK MANAGEMENT

9.1. Identification of a customer is important pre-requisite for opening an account. Non-adherence of this may lead to the risks viz. frauds, money laundering, inadvertent overdrafts, Benami / fictitious accounts.

9.2. Non-compliance of monitoring of the transactions exceeding the threshold limit and non-recording of the transactions may result in intentional splitting/structuring of transaction to evade taxes, money laundering and financing of terrorist activities.

9.3. **Risk Categorization of Customers**

Customers shall be categorized as low, medium and high risk category, based on the assessment and risk perception. The branches should prepare the profile of the customer which should contain information relating to customers' identity, social/financial status, nature of business activity, information about his clients' business and their location etc. and risk categorization shall be undertaken based on these parameters. While considering customer's identity, the ability to confirm identity documents through online or other services offered by the issuing authorities may also be factored in. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes without the express permission of the customer. The customer profile shall be prepared based on risk categorization, as defined below:

9.3.1 Low Risk Category: 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.

Example:

a) Salaried Employees, whose salary structures are well defined,
b) People belonging to lower economic strata of the Society whose accounts show small balances and low turnover,
c) Government departments and Government owned Companies, Regulators and statutory bodies etc.
d) All other Customers who are not classified as High Risk or Medium Risk Categories

For low risk category customers, only the basic requirements of verifying the identity and location of the customer are to be obtained. However, whenever there is suspicious of money laundering or terrorist financing or when other factors give rise to a belief that the customer does not, in fact pose a low risk, full scale customer due diligence should be carried out before opening an account or whenever such risk perceived.

9.3.2 **Medium Risk Category:** are those individuals who live in Medium risk Countries i.e. all Countries in Africa and all countries in the America other than USA and Canada and Such customers who possess lower risk than 'High Risk Customers' but higher than the 'Low Risk Customers' based on their background, nature and location of activity, country of origin, sources of funds etc. The Risk Classification may be lower for those customers where

sufficient knowledge in the public domain is available to Bank (e.g. listed companies, Regulated Entities).

INDICATIVE LIST OF MEDIUM RISK CUSTOMERS

i. Non-Bank Financial Institution
ii. Stock brokerage
iii. Import / Export
iv. Gas Station
v. Car / Boat / Plane Dealership
vi. Electronics (wholesale)
vii. Travel agency
viii. Used car sales
ix. Telemarketers
x. Providers of telecommunications service, internet café, IDD call service, phone cards, phone center
xi. Dot-com company or internet business
xii. Pawnshops
xiii. Auctioneers
xiv. Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.
xv. Sole Practitioners or Law Firms (small, little known)
xvi. Notaries (small, little known)
xvii. Secretarial Firms (small, little known)
xviii. Accountants (small, little known firms)
xix. Venture capital companies

9.3.3 **<u>High Risk Category</u>**: Individuals and entities whose identities and sources of funds are not clear and cannot be easily identified.

Example:

a. Non-resident customers and Foreign Nationals residing / hailing from High Risk Countries.
b. High Net Worth individuals (HNIs) – as defined under para 3.1.2.9.
c. Trusts, Charities, NGOs and Organizations receiving donations (especially those operating on a ―cross border basis) unregulated clubs and organizations receiving donations. However, NPOs/NGOs promoted by United Nations or its agencies may be classified as low risk customers.
d. Companies having close family shareholding or beneficial Ownership
e. Firms with 'Sleeping Partners'
f. Politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which PEP is the ultimate beneficial owner;

g. Non face to face customers and
h. Those with dubious reputation as per public information available etc.
i. Customers dealing in antique goods
j. Money Exchange Bureaus
k. Diamond, Bullion Dealers & Jewelers.
l. Arms and Ammunition dealers.

Additional indicative list of High Risk Customers:

i. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UNSC 1267 & 1988 [2011] linked to Al Qaida & Taliban.
ii. 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
iii. Individuals and entities in watch lists issued by Interpol and other similar international organizations
iv. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk
v. 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.
vi. Customers based in high risk countries/jurisdictions or locations as identified by FATF from time to time.
vii. Accounts of Embassies / Consulates;
viii. Off-shore (foreign) corporation/business
ix. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
x. 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
xi. Investment Management / Money Management Company/Personal Investment Company
xii. 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.
xiii. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc
xiv. Money transfer Service Business: including seller of: Money Orders / Travelers‟ Checks / Money Transmission /Check Cashing / Currency Dealing or Exchange

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

xvi. Gambling/gaming including ―Junket Operators‖ arranging gambling tours

xvii. 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).

xviii. Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries.

xix. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.

xx. Customers that may appear to be Multi-level marketing companies etc.

9.3.4 For High Risk Category & Medium Risk Category customers, the Enhanced Due Diligence (EDD) be done by taking the information such as customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. should be obtained. There should be periodical review of risk categorization of accounts followed by enhanced due diligence measures. Such review of risk categorization of customers should be carried out at least once in every six months.

9.3.5 Branch may take a view on risk categorization of each customer into low, medium and high risk category depending on their experience, expertise in profiling of the customer based on their understanding, judgment, assessment and risk perception of the customer and not merely based on any group or class they belong to.

9.3.6 It should be noted that Banking Services are not denied to general public, especially to those who are financially or socially disadvantaged.

Explanation: FATF Public statement, the reports and guidance notes on KYC/AML issued by the Indian Bank Association (IBA) may also be used in risk assessment.

9.4 ML/TF Risk Calcification of PRODUCTS & SERVICES

Nature of Service	Products/ services	Risk Classification
Retail Banking	Deposit Accounts - Savings, Current & Time Deposits	Low
	Current Accounts for Proprietor & Partnerships	Low
	Investment Account - Fixed, Recurring	Low
	Demand loan, cash credit, Over drafts, Term loans	Low
	Personal Loans,	Medium
	Home Loan	Low
	Vehicle Loan	Low
	Commercial Loan	Medium
	Working Capital Loan	Low
	Asset based lending	Medium
	Debit/ Stored value or Prepaid cards	Low
	Safe Deposit Box, Safe Deposit Lockers	Medium
	Lending activities, particularly loans secured by cash collateral and marketable securities	Medium
Treasury Services	Debt Instruments (commercial paper, certificate of deposits, preferential shares, debentures, securitized participation, interbank participation or any other investments in securities)	High
	Bullion	High
	IPO Underwriting services	High
Wealth Management	Overnight investment accounts (sweep accounts)	High
	Trust and Asset management services	High
	Securities Account (Demat) & S	Medium
Wholesale Banking	Bill Discounting	High
	Foreign Bank Guarantee (FBG)	High
	Foreign Cheque Collection (FCC)	High
	Export (Inward) LC	High
	Packing Credit	High
	Foreign LC, Foreign LC- Amendment	High
	Standby Letter of credit/ Letter of comfort	High
	Special use or concentration accounts	High
	Project financing & Trade financing for sensitive industries in high-risk jurisdictions	High
Private Banking	Wealth Management services to HNIs	High
	Non-deposit account services such as Non-deposit investment products and Insurance	
Remittance Services	Electronic funds payment services such as Electronic Debit/ Credit Cards (e.g., Both Prepaid and post-paid cards), funds transfers	Medium

	(domestic and international), etc.	
	Electronic banking such as Internet Banking, Mobile Banking & Phone Banking etc.	Medium
	Foreign correspondent Bank accounts & Services offering anonymity or involving third parties.	Medium
	Currency exchange transactions, Services offering cash, monetary or bearer instruments; cross-border transactions, etc.,	High
	Services offering anonymity or involving third parties and walking customers	High
	Services involving banknote and precious metal trading and delivery	

9.5 **INDICATIVE LIST OF HIGH / MEDIUM/ LOW RISK GEOGRAPHIES/ LOCATIONS/ COUNTRIES:** Please refer for **t**he list of Countries with risk classification is annexed as Annexure – VII.

9.5.1 Countries/Jurisdictions

i. Countries subject to sanctions, embargoes or similar measures in the United Nations Security Council Resolutions (―UNSCR‖).
ii. Jurisdictions identified in FATF public statement as having substantial money laundering and terrorist financing (ML/FT) risks (www.fatfgafi.org)
iii. Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies (www.fatf-gafi.org)
iv. Tax havens or countries that are known for highly secretive banking and corporate law practices
v. Countries identified by credible sources 1 as lacking appropriate AML/CFT laws, regulations and other measures.
vi. Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organizations operating within them.
vii. Countries identified by credible sources as having significant levels of criminal activity.
viii. 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).

9.5.2 Locations

i. Locations within the country known as high risk for terrorist incidents or terrorist financing activities (e.g. sensitive locations in Jammu and Kashmir, North east, Naxal affected districts)
ii. Locations identified by credible sources as having significant levels of criminal, terrorist, terrorist financing activity.
iii. Locations identified by the bank as high-risk because of its prior experiences, transaction history, or other factors.

9.5.3. INDICATIVE LIST OF HIGH RISK COUNTRIES: The countries identified by Financial Action Task Force [FATF] as high risk countries which continue to show deficiencies in their Anti Money Laundering and Combating of Financing of Terrorism framework will be circulated from time to time. The list of countries with Risk clarification is provided in Annexure-VII.

9.6. The indicative list of parameters for risk categorization has been expanded to include geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken, etc. Branch shall treat the risk categorization and reasons for risk categorization of customers as confidential.

9.7 ML/TF Risk classification of various types of Transactions:

ML/TL Risk Classification for Transactions	
Type of Transaction	Risk Classification
Cash transactions	High
Cheque, payment order or other instruments	Low
Issuing and cashing of Travellers cheques	Low
Debit card & Credit card transactions	Low
Merchant point of sales (POS) for Debit & Credit Card	Low
Foreign exchange services- Cash/ Cheque OTC	High
Foreign exchange services- Inter account transfer	Low
Mobile banking services	Low
Internet banking	Low
Domestic wire transfer/ electronic funds transfer services	Low
International wire transfer/ electronic fund transfer services	High

9.8 ML/TF Risk classification of Channels:

Channel	Risk classification
Face to Face Customer (Branch on-boarding)	Low
Business Correspondents (BC)	Low
Video KYC (online On-boarding)	Low
Customer on-boarding in face to face mode	Low
Non Face to face customer (Accounts opened using Aadhaar OTP in digital mode)	High
Non Face to face customer on-boarding(Non account based Customer) channel	High

10. INTERNAL CONTROL

To avoid such risks, Zonal / Regional Offices should put in place proper monitoring machinery to ensure that the branches are meticulously following the laid down guidelines/procedures with regards to KYC norms and Money Laundering activities.

10.1 Internal Audit/Inspection

10.1.1 Internal Auditors/Concurrent Auditors will carry out an independent evaluation of the controls, for identifying high value transactions.

10.1.2 Concurrent/internal auditors will verify the compliance with KYC/AML policies and procedures. They will specifically scrutinize and comment on the observance of KYC norms and the steps taken towards prevention of Money Laundering by the Branches. As per the directions of DFS, GOI, 1% of the new accounts opened during the month/audit period be got verified by the Auditors by reaching out to the new customers.

10.1.3 All accounts opened through V-CIP shall be made operational only after being subject to audit, to ensure the integrity of process. To ensure security, robustness and end to end encryption, software and security audit and validation of the V-CIP application shall be carried out before rolling it out in the branches.

10.1.4 Develop a system of audit for the IT framework and compliance with Rules 114F, 114G and 114H of Income Tax Rules with regards to FATCA / CRS.

10.2. Terrorism Finance:

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, terrorists acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

10.2.1 Reserve Bank of India/Government of India/Central Office from time to time is communicating the list of individuals/entities of terrorist organization/Banned organization etc. Branches should update the list and exercise care while dealing with such entities/organization.

10.2.2 Branches should keep a watchful eye on the transactions of the terrorist organizations listed in the ordinance, accounts of individuals and entities listed by the Security Counsel of Sanctions Committee of the UN. Violations of the extant acts or normal banking operations must be reported to the appropriate authorities under the ordinance.

10.3 Fixation of Annual Threshold limits for financial transactions in various account relationships of Customers:

10.3. (a) At the beginning of the financial year, threshold limits is required to be fixed @ five (5) times of declared annual income, for all existing accounts & @ five (5) times of declared annual income on pro-rata basis, in case of new accounts opened in the middle of the financial year.

10.3. (b) These Threshold limits will be reviewed annually at the start of financial year by system based updated Annual income/ Annual Business turnover declared by the Customer during periodic Updation of KYC.

10.3. (c) Besides the above criteria, wherever any regulatory direction is in place, the same has to be complied with. Further it is desirable to restrict transactions in accounts opened in the name of certain type of Customers, such as Housewives, Students, Minors, PMJDY Customers, Labourers in un-organised sector, whose source and quantum of income is not ascertainable or not known to the Bank based on I.T Returns or other reliable sources. The maximum annual Threshold limits proposed are as under:

i. Small Accounts (Accounts without OVD): Rs.100,000/-.
ii. Accounts opened with Aadhaar OTP in non-face-to-face mode: Rs. 2,00,000/-
iii. PMJDY accounts: Rs.5,00,000/-
iv. BSBD General accounts: Rs.500,000/-
v. Accounts of Students, House wife, Minor and Labourers working in Un-organized sectors: Rs. 10,00,000/- in case of SB accounts and Rs. 25,00,000/- in case of Current accounts.

10.3.(d) The main objective for having above annual Threshold limits is based the past experience of awards imposed by various Banking Ombudsmen (BOs) and also to comply with MF/TF Risks involved and to prevent misuse of Bank accounts opened in the name of Housewives, Students, Minors, PMJDY Customers, Labourers in un-organized sector as Money Mules.

10.3.1 STR reported accounts

Our Bank's KYC instructions stipulate "The accounts reported in STR bears a high degree of Risk and these accounts are subject to enhanced monitoring. If significant activities are observed in these accounts a repeat STR may also be filed. The competent authority should take a decision for closure of such an account/s where STR is repeatedly reported. However such customer should not be tipped off.

Looking to the potential risk in such accounts, Zonal Manager of the zone is designated as the appropriate authority to take decision for closure of such account in which more than **THREE** STRs have been filed.

10.4 Scenarios for generation of STR alerts:

64 minimum common scenarios (37 Short term and 27 Medium term) for generation of STR alerts through system and an indicative list of 27 offline alerts which are to be scrutinized by the branches, suggested by IBA/RBI, be followed for effective control/monitoring and reporting of Suspicious Transaction Reports (STR). The front line staff at branches should be vigilant, as they are the first point to detect any suspicious transaction in an account and accordingly any suspicious transaction/activity should immediately be reported to the Regulatory Authorities through the Compliance Officer at ROs/Principal Officer of our Bank.

10.5. Preservation of Record/ Record Management

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

10.5.1 All financial transactions records including credit/debit slips, cheques and other forms of vouchers etc., (for account holders and walk-in-customers i.e., non-account holders) for both domestic and international should be maintained/ retained for at least five years from the date of transaction between clients and banking company and in terms of sub-section 2(b) of section 12 of the PML Act, the records referred to in clause(c) of subsection(1) of section12 shall be maintained for a period of five years from the date of cessation of transaction between the clients and the banking company and should be available for perusal and scrutiny of audit functionaries as well as regulators as and when required.

10.5.2 In case of wire transfer/Electronic Funds Transfer transaction, the records of electronic payments and messages must be treated in the same way as other records in support of entries in the account.

10.5.3 Branches should ensure that records pertaining to the identification of the customers and their address (e.g. copies of documents like aadhaar, passports, identity cards, driving licenses, PAN, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended.

10.5.4 Branches should maintain for at least five years from the date of transaction between the bank and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the nature of transactions, date on which the transaction was conducted, parties to the transaction, the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

10.5.5 The term “cessation” would broadly mean the closure of the account. However, there may be certain exceptions to this e.g.

10.5.5.1 If the matter related to a suspicious transaction is pending in a Court, the relevant records should be retained for 10 years from the date of final verdict of the Court.

10.5.5.2In specific cases, where RBI/FIU-IND or any other regulatory body requests for the retention of the records for a period more than 10 years, branches should be guided by such requests.

10.5.6 The records pertaining to transaction and identification as mentioned above should be made available to the competent authorities upon request. The expressions "records pertaining to the identification", “identification records”, etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

10.5.7: Branches should make available swiftly, the identification records and transaction data to the competent authorities upon request by introducing 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);

10.5.8: Branches should 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.

10.5.09: Branches should 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;

10.5.10: Branches are required to maintain records of identity and address of their customers and records in respect of transactions referred in Rule 3 of PMLA in hard and soft format.

10.5.11: In case of customers who are non-profit organizations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If such customers are not registered, the Branch shall register the details on the DARPAN Portal. Branches shall also maintain such registration records for a period of five years after the business relationship between the Customer and the Branch has ended or the account has been closed, whichever is later.

10.6. COMPLIANCE OFFICER/MONEY LAUNDERING REPORTINGOFFICER (MLRO)

10.6.1 The Zonal/Regional offices should designate a senior most officer not below the rank of Chief Manager, to act as Compliance Officer. The branches will report the suspicious transactions to the Compliance Officer immediately, who will investigate the suspicious transactions and report the same to the Principal Officer.

10.6.2 COMPLIANCE OFFICER will initiate follow up action on unusual or suspicious activity and co-ordinate with branch functionaries in deciding on the desirability of continuing the account with increased caution and monitoring or to close the account.

10.6.3 The COMPLIANCE OFFICER will analyze the suspicious activities reported and track patterns, which should be brought to the notice of the operating staff. This will enable the staff to remain vigilant against similar transactions.

10.6.4 Regional Offices will designate officers as Money Laundering Reporting Officer (MLRO) for scrutiny of STR alerts in case the STR alerts are decentralized for scrutiny at Regional Office level. The MLRO will submit the report of scrutinized alerts to Compliance Officer at ROs for further Scrutiny and onward submission to Central Office.

10.7 Hiring of Employees:

a. Adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of their personnel recruitment/hiring process shall be put in place.
b. Bank should endeavour to ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have: high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally.
c. Bank should also strive to develop an environment which fosters open communication and high integrity amongst the staff.

10.8 Employee training:

On-going employee training programme are put in place so that the members of staff are adequately trained in KYC/AML/CFT policy. The focus of the training is different for frontline staff, compliance staff, risk management staff, staff working in capital market related services, Depository participants services, Audit staff and staff dealing with new customers. The front desk staffs are trained to handle issues arising from lack of customer education. Staff training colleges / centers are ensuring compliance in the matter. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies, regulation and related issues also ensures its proper implementation.

E-Learning module through Cent Swadhyay has been introduced for increased awareness.

10.9 Customer Education:

Implementation of AML/CFT measures requires Banks to demand certain information from customers which may be of personal nature or has hitherto never been called for. Such information can include documents evidencing source of funds/ income tax returns etc., this can sometimes lead to raising of questions by the customers with regard to the motive and purpose of collecting such information. There is, therefore, a need for Banks to sensitize their customers about these requirements as the ones emanating from AML and CFT frame work. Banks shall prepare specific literature/ pamphlets etc. so as to educate the customer\s of the objectives of AML/ CFT procedures.

****

ANNEXURE- I:

Digital KYC Process

A. The application for digital KYC process which shall be made available at customer touch points for undertaking KYC of the 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 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 to its authorized officials. C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the branch or vice-versa. The original OVD shall be in possession of the customer.

C. It must be 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 shall put a watermark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by Bank) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

D. The Application 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.

E. 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.

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

G. 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.

H. 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 shall not be used for customer signature. There must be a check put in place that the mobile number used in customer signature shall not be the mobile number of the authorized officer.

I. 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.

J. 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 branch, 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.

K. The authorized officer of the shall check and verify that:-
   1. information available in the picture of document is matching with the information entered by authorized officer in CAF.
   2. live photograph of the customer matches with the photo available in the document.; and
   3. all of the necessary details in CAF including mandatory field are filled properly.;

L. On Successful verification, the CAF shall be digitally signed by authorized officer of the 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.

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

****

ANNEXURE- II

KNOW YOUR CUSTOMER (KYC) GUIDELINES: ANTI-MONEY LAUNDERING (AML) STANDARDS

KNOW YOUR CUSTOMER (KYC)			
Sr. No.	**DO's**	**Sr. No.**	**DON'Ts**
1	Before opening any new account, it is ensured that the prospective account opener's identity does not match with any person with known criminal background, and his name does not appear in the list of terrorist individuals/ organizations banned by UN Security Council Sanction Committee as circulated by RBI.	1	Do not open account in anonymous or fictitious / benami name(s).
2	All the copies of supporting documents given by the customer must be verified with original documents.	2	Do not open account where branch is unable to apply appropriate Customer Due Diligence (CDD) measures either due to non-cooperation of the customer or non – reliability of the documents / information furnished by the customer.
3	Circumstances in which a customer is permitted to act on behalf of another person / entity is clearly spelt out.	3	Do not accept new customer for banking relationship without application of CDD measures such as location of business activity / profession, purpose of the account, social and financial status source of funds etc.
4	Where PAN is obtained, the same shall be verified from the verification facility of the issuing authority.	4	Do not open any account without PAN or the equivalent e-document thereof or Form 60, a photograph and such other documents including in respect of financial status of the customer, or the equivalent e-documents thereof as may be required along with Proof of Identity and Address. Individuals –aadhaar or an officially valid document or the equivalent e-document thereof containing the details of his identity and address from the following: Passport, Driving License, Voter ID, Job Card issued by NREGA duly signed by officer of State Govt., Letter issued by the National Population Register or any document as notified by the Central Government in consultation with the regulator. Sole Proprietary Firm: Do not open account without CCD procedure of the proprietor along with any two documents or the equivalent e-document there of as a proof of business / activity in the name of the proprietary firm- Registration certificate, Certificate/ license issued by the municipal authorities under Shop and Establishment Act, Sales and income tax returns, CST/VAT/ GST certificate (provisional / final) , Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities, 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, 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

			or Utility bills such as electricity, water, landline telephone bills, etc. Partnership Firm – Registration certificate, Partnership Deed, Permanent account number of the Partnership firm and documents specified for CDD procedure for individuals and includes obtaining aadhaar or any officially valid document or the equivalent e-document thereof containing the details of proof of identity and address, one recent photograph and Permanent Account Number (PAN) or the equivalent e-document thereof or Form 60 relating to the beneficial owner, managers, officers or employees holding an attorney to transact on its behalf. Companies – Certificate of Incorporation, Memorandum and Articles of Association, Permanent account number of the company, Resolution of Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf along with documents specified for CDD procedure for individuals relating to the beneficial owner, for proof of identity and proof of address of managers, officers or employees holding an attorney to transact on its behalf. Trusts &Foundations-Registration certificate, Trust Deed, Permanent account number of Form 60 of the trust along with documents specified for CDD procedure for individuals relating to the beneficial owner for proof of identity and proof of address of the person holding a power of attorney to transact on its behalf. Unincorporated Association or Body of Individuals-Resolution of the managing body of such association or body of individuals, Permanent account number or Form 60 of the Unincorporated Association or Body of Individuals, Power of attorney granted to transact on its behalf along with documents specified for CDD procedure for individuals relating to the beneficial owner for proof of identity and proof of address of the person holding an attorney to transact on its behalf and any such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals. Juridical Persons: Government or its department, Societies, Universities and Local bodies like Village Panchayats - Documents showing name of person authorized to act on behalf of the entity; along with documents specified for CDD procedure for individuals relating to the beneficial owner for proof of identity and address in respect of the person holding an attorney to transact on its behalf and Such documents as may be required by the branch to establish the legal existence of such an entity / juridical person.
5	All transactions of suspicious nature, should be monitored	5	Do not open an account without : Proof of either current or permanent address And the officially valid documents for proof of address and proof of identity.
6	High risk accounts are subject to intensive monitoring and special	6	In the case of 'Small Accounts', if the balance (in all the accounts taken together) exceeds Rs. 50,000/- or total credits

	attention is paid to all complex, usually large transactions which have no economical / lawful purpose.		(in all the accounts taken together) exceeds Rs. One lac in a year, or aggregate of all withdrawals and transfers in a month exceeds Rs. Ten thousand then do not permit further transactions in the account until full KYC procedure is completed.
7	Based on the risk perception, every new customer should be categorized into low, medium or high risk for monitoring purpose. Risk profiles of customers should be reviewed, once in every six months.	7	Banking services should not be denied to general public, especially, to those who are financially or socially disadvantaged.
8	Periodical updation of KYC information of every customer (including photographs) should be done every Two years for High Risk customers, every Eight years for Medium Risk customers and every Ten years for Low Risk customers.	8	In the accounts where a Suspicious Transaction Report (STR) has been made no restriction are put on the operations and it is ensured that there is no tipping off to the customers.
9	Ensure that all the transactions where any forgery of a valuable security or a document has taken place facilitating the transactions are reported to Zonal Office within 3 days for submission by H.O. to Financial Intelligence Unit – India (FIU-IND), New Delhi.	9	Do not open new NRI accounts without a. Passport for verification with a copy. b. Work permit / permanent residency / Green Card etc. indicating the NRIs residential status abroad for verification with copy. c. NRI Declaration.
10	Demand Draft/Pay Order/mail transfer for Rs. 50,000/- and above is issued only by debit to customers account or against cheque and not against cash		
11	In case of all domestic inward remittances of Rs. 50,000/- and above and all foreign inward remittance of any amount, beneficiary account is credited only when complete originator information i.e. name, address and account number is available or after receipt of the originator information.		
12	Proper record of all transactions reported to ZO/HO in CCR and STR formats are maintained/ preserved for a period of at least 5 years from the date of cessation of each such transaction.		
13	CDD Procedure is to be followed for all the joint account holders, while opening a joint account.		
14	Where an equivalent e-document is obtained from the customer, branches shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).		

ANNEXURE- III

For the benefit of all the offices, we are giving hereunder sample of GROUNDS OF SUSPICION reported in STRs

No.	Suspicion	Summary of detection and review
1	False Identity	Identification documents were found to be forged during customer verification process. The account holder was not traceable.
2	Wrong Address	Welcome kit was received back as the person was not staying at the given address or address details given by the account holder were found to be false. The account holder was not traceable.
3	Doubt over the real beneficiary of the account	The customer not aware of transactions in the account. Transactions were inconsistent with customer's profile.
4	Account of persons under investigation	The customer was reported in media for being under investigation.
5	Account of wanted criminal	Name of the account holder and additional criteria (Date of birth/Father's name/Nationality) were same as a person on the watch list of UN, Interpol etc.
6	Account used for cyber crime	Complaints of cyber-crime were received against a customer. No valid explanation for the transactions by account holder.
7	Account used for lottery fraud	Complaints were received against a bank account used for receiving money from the victims. Deposits at multiple locations followed by immediate cash withdrawals using ATMs. No valid explanation provided by the account holder.
8	Doubtful activity of a customer from high risk country	Cash deposited in a bank account at different cities on the same day. The account holder, a citizen of a high risk country with known cases of drug trafficking.
9	Doubtful investment in IPO.	Large number of accounts involving common introducer or authorized signatory. Accounts used for multiple investments in IPOs of various companies.
10	Unexplained transfers between multiple accounts.	Large number of related accounts with substantial inter-account transactions without any economic rationale.
11	Unexplained activity in dormant accounts	Sudden spurt in activity of dormant account. The customer could not provide satisfactory explanation for the transactions.
12	Unexplained activity in account inconsistent with the declared business	Transactions in account inconsistent with what would be expected from declared business. The customer could not provide satisfactory explanation.
13	Unexplained large value transactions inconsistent with client's apparent financial standing	Large value transactions in an account which usually has small value transactions. No valid explanation provided by the account holder.

No.	Suspicion	Summary of detection and review
14	Doubtful source of payment for credit card purchases	Credit card topped up by substantial cash first and then used for incurring expenses. Cumulative payment during the year was beyond known source of income.
15	Suspicious use of ATM card.	Frequent cash deposits in the account followed by ATM withdrawals at different locations. No valid explanation.
16	Doubtful use of safe deposit locker	Safe deposit locker operated frequently which is inconsistent with the financial status of client.
17	Doubtful source of cash deposited in bank account	Frequent cash transactions of value just under the reporting threshold. Cash transactions split across accounts to avoid reporting. No valid explanation provided.
18	Suspicious cash withdrawals from Bank account.	Large value cheques deposited followed by immediate cash withdrawals.
19	Doubtful source of foreign inward transfers in bank account	Deposit of series of demand drafts purchased from Exchange House abroad. Sudden deposits in dormant account immediately followed by withdrawals.
20	Doubtful remitter of foreign remittances	Name and other details of the remitter matches with a person on watch list.
21	Doubtful beneficiary of foreign remittances	Name and other details of the beneficiary matches with a person on watch list.
22	Doubtful utilizations of foreign remittances	Foreign remittance being withdrawn in cash immediately. No valid explanation.
23	Misappropriation of funds	Reports of misappropriation of funds. Substantial cash withdrawals in account of a charitable organization.

Annexure-IV

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: 011-23092456, 011-23092465 (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-mhaqov.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: isctcr-mhaAgov.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) **and any other person:**

(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.

(a) The DNFBPs are required to ensure that if any designated individual/entity approaches them for a transaction or relationship or attempts to undertake such transactions, the dealer should not carry out such transactions and, without delay, inform the UAPA Nodal officer of the State/UT with details of the funds/assets held and the details of the transaction, who in turn would follow the same procedure as in para 6.2 to 6.6 above. Further, if the dealers hold any

assets or funds of the designated individual/entity, either directly or indirectly, they shall freeze the same without delay and inform the UAPA Nodal officer of the State/UT.

(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.

(ix) Any person, either directly or indirectly, holding any funds or other assets of designated individuals or entities, shall, without delay and without prior notice, cause to freeze any transaction in relation to such funds or assets, by immediately informing the nearest Police Station, which shall, in turn, inform the concerned UAPA Nodal Officer of the State/UT along with the details of the funds/assets held. The concerned UAPA Nodal Officer of the State/UT, would follow the same procedure as in para 6.2 to 6.6 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 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 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.

11A. Regarding procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/organizations in the event of delisting by the UNSCR 1267 (1999), 1988 (2011) and 1989 (2011) Committee.

Upon making an application in writing by the concerned individual/organization, to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, RoC, Regulators of DNFBPs, Department of Posts and the UAPA Nodal Officers of all States/UTs., who in turn shall forward the application along with the full details of the assets frozen to the Central [Designated] Nodal Officer for UAPA within two working days. The Central [Designated] Nodal Officer for UAPA shall examine the request in consultation with the Law Enforcement Agencies and other Security Agencies and Intelligence Agencies and cause such verification as may be required and if satisfied, shall pass an order, without delay, unfreezing the funds, financial assets or economic resources or related services owned or held by the applicant under intimation to concerned bank, stock exchanges/ depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties, RoC, Regulators of DNFBPs, Department of Posts and the UAPA Nodal Officers of all States/UTs

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.

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

To,

1. Governor, Reserve Bank of India, Mumbai
2. Chairman, Securities & Exchange Board of India, Mumbai
3. Chairman, Insurance Regulatory and Development Authority, Hyderabad.
4. Foreign Secretary, Ministry of External Affairs, New Delhi.
5. Finance Secretary, Ministry of Finance, New Delhi.
6. Revenue Secretary, Department of Revenue, Ministry of Finance, New Delhi.
7. Secretary, Ministry of Corporate Affairs, New Delhi
8. Chairman, Central Board of Indirect Taxes & Customs, New Delhi.
9. Director, Intelligence Bureau, New Delhi.
10. Additional Secretary, Department of Financial Services, Ministry of Finance, New Delhi.
11. Chief Secretaries of all States/Union Territories
12. Principal Secretary (Home)/Secretary (Home) of all States/ Union Territories
13. Directors General of Police of all States & Union Territories
14. Director General of Police, National Investigation Agency, New Delhi.
15. Commissioner of Police, Delhi.
16. Joint Secretary (Foreigners), Ministry of Home Affairs, New Delhi.
17. Joint Secretary (Capital Markets), Department of Economic Affairs, Ministry of Finance, New Delhi.
18. Joint Secretary (Revenue), Department of Revenue, Ministry of Finance, New Delhi.
19. Director (FIU-IND), New Delhi.

Copy for information to: -

1. Sr. PPS to HS
2. PS to SS(IS)

ANNEXURE-V

F.No.P2011/14/2022-ESCell-DOR
Government of India
Ministry of Finance
Department of Revenue

New Delhi, dated the 1st September, 2023.

ORDER

Subject: - Procedure for implementation of Section 12A of "The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005".

Section 12A of The Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 [hereinafter referred to as 'the Act'] reads as under: -

"12A. (1) No person shall finance any activity which is prohibited under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.

(2) For prevention of financing by any person of any activity which is prohibited under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems, the Central Government shall have power to—

a) freeze, seize or attach funds or other financial assets or economic resources—

i. owned or controlled, wholly or jointly, directly or indirectly, by such person; or
ii. held by or on behalf of, or at the direction of, such person; or
iii. derived or generated from the funds or other assets owned or controlled, directly or indirectly, by such person;

prohibit any person from making funds, financial assets or economic resources or related services available for the benefit of persons related to any activity which is prohibited under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems.

(3) The Central Government may exercise its powers under this section through any authority who has been assigned the power under sub-section (1) of section 7."

II In order to ensure expeditious and effective implementation of the provisions of Section 12A of the Act, the procedure is outlined below.

1. Appointment and communication details of Section 12A Nodal Officers:

1.1 In exercise of the powers conferred under Section 7(1) of the Act, the Central Government assigns Director, FIU-India, Department of Revenue, Ministry of Finance, as the authority to exercise powers under Section 12A of the Act. The Director, FIU-India shall be hereby referred to as the Central Nodal Officer (CNO) for the purpose of this order. [Telephone Number: 011-23314458, 011-23314435, 011-23314459 (FAX), email address: dir@fiuindia.gov.in].

1.2 Regulator under this order shall have the same meaning as defined in Rule 2(fa) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. Reporting Entity (RE) shall have the same meaning as defined in Section 2 (1) (wa) of Prevention of Money-Laundering Act, 2002. DNFPBs is as defined in section 2(1) (sa) of Prevention of Money-Laundering Act, 2002.

1.3 The Regulators, Ministry of Corporate Affairs and Foreigners Division of MHA shall notify a Nodal Officer for implementation of provisions of Section 12A of the Act. The Regulator may notify the Nodal Officer appointed for implementation of provisions of Section 51A of UAPA, also, as the Nodal Officer for implementation of Section 12A of the Act. All the States and UTs shall notify a State Nodal officer for implementation of Section 12A of the Act. A State/UT may notify the State Nodal Officer appointed for implementation of provisions of Section 51A of UAPA, also, as the Nodal Officer for implementation of Section 12A of the Act.

1.4 The CNO shall maintain an updated list of all Nodal Officers, and share the updated list with all Nodal Officers periodically. The CNO shall forward the updated list of all Nodal Officers to all REs.

2. Communication of the lists of designated individuals/entities:

2.1 The Ministry of External Affairs will electronically communicate, without delay, the changes made in the list of designated individuals and entities (hereinafter referred to as 'designated list') in line with section 12A (1) to the CNO and Nodal officers.

2.1.1 Further, the CNO shall maintain the Designated list on the portal of FIU-India. The list would be updated by the CNO, as and when it is updated, as per para 2.1 above, without delay. It shall make available for all Nodal officers, the State Nodal Officers, and to the Registrars performing the work of registration of immovable properties, either directly or through State Nodal Officers, without delay.

2.1.2 The Ministry of External Affairs may also share other information relating to prohibition / prevention of financing of prohibited activity under Section 12A (after its initial assessment of the relevant factors in the case) with the CNO and other organizations concerned, for initiating verification and suitable action.

2.1.3 The Regulators shall make available the updated designated list, without delay, to their REs. The REs will maintain the designated list and update it, without delay, whenever changes are made as per para 2.1 above.

2.2 The Nodal Officer for Section 12A in Foreigners Division of MHA shall forward the updated designated list to the immigration authorities and security agencies, without delay.

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

3.1 All Financial Institutions shall –

i. Verify if the particulars of the entities/individual, party to the financial transactions, match with the particulars of designated list and in case of match, REs shall not carry out such transaction and shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the CNO by email, FAX and by post, without delay.

ii. Run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial assets or economic resources or related services, in the form of bank accounts, stocks, Insurance policies etc. In case, the particulars of any of their customers match with the particulars of designated list, REs 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 on their books to the CNO by email, FAX and by post, without delay.

iii. The REs shall also send a copy of the communication, mentioned in 3.1 (i) and (ii) above, to State Nodal Officer, where the account/transaction is held, and to their Regulator, as the case may be, without delay.

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

3.2 On receipt of the particulars, as referred to in Paragraph 3.1 above, the CNO 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 REs are the ones in designated list and the funds, financial assets or economic resources or related services, reported by REs are in respect of the designated individuals/entities. This verification would be completed expeditiously from the date of receipt of such particulars.

3.3 In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under Section 12A would be issued by the CNO without delay and be conveyed electronically to the concerned RE under intimation to respective Regulators. The CNO shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and All 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. The CNO

shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating suitable action.

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

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

4.1 The Registrars performing work of registration of immovable properties shall --

i. Verify if the particulars of the entities/individual, party to the transactions, match with the particulars of the designated list, and, in case of match, shall not carry out such transaction and immediately inform the details with full particulars of the assets or economic resources involved to the State Nodal Officer, without delay.
ii. Verify from the records in their respective jurisdiction, without delay, on given parameters, if the details match with the details of the individuals and entities in the designated list. 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 Registrar shall immediately inform the details with full particulars of the assets or economic resources involved to the State Nodal Officer, without delay.
iii. In case there are reasons to believe beyond doubt that assets that are held by an individual/entity would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A, Registrar shall prevent such individual/entity from conducting transactions, under intimation to the State Nodal Officer by email, FAX and by post , without delay.

4.2 the State Nodal Officer would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources to the CNO without delay by email, FAX and by post.

4.3 The State Nodal Officer may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent 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 CNO without delay by email, FAX and by post.

4.4 The CNO may also have the verification conducted by the Central Agencies. This verification would be completed expeditiously.

4.5 In case, the results of the verification indicate that the assets are owned by, or are held for the benefit of, the designated individuals/entities, an order to freeze these assets under Section 12A would be issued by the CNO without delay and be conveyed electronically to the concerned Registrar performing the work of registering immovable properties, and to FIU under intimation to the concerned State Nodal Officer. The CNO shall also forward a copy thereof to all the Principal Secretaries/Secretaries, Home Department of the States/UTs and All 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. The CNO shall also forward a copy of the order to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating suitable action.

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

5. Regarding the real-estate agents, dealers of precious metals/stones (DPMS), Registrar of Societies/ Firms/ non-profit organizations, The Ministry of Corporate Affairs and Designated Non-Financial Businesses and Professions (DNFBPs):

(i) The dealers of precious metals/stones (DPMS) as notified under PML (Maintenance of Records) Rules, 2005 and Real Estate Agents, as notified under clause (vi) of Section 2(1) (sa) of Prevention of Money-Laundering Act, 2002, are required to ensure that if any designated individual/entity approaches them for sale/purchase of precious metals/stones/Real Estate Assets or attempts to undertake such transactions, the dealer should not carry out such transaction and, without delay, inform the Section 12A Nodal officer in the Central Board of Indirect Taxes and Customs (CBIC). Also, If the dealers hold any assets or funds of the designated individual/entity, they shall freeze the same without delay and inform the Section 12A Nodal officer in the CBIC, who will, in turn, follow procedure similar to as laid down for State Nodal Officer in the paragraphs 4.2 to 4.6.

(ii) Registrar of Societies/ Firms/ non-profit organizations are required to ensure 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 shall freeze any transaction for such designated individual/ entity and shall inform the State Nodal Officer, without delay, and, if such society/ partnership firm/ trust/ non-profit organization holds funds or assets of designated individual/ entity, follow the procedure as laid down for State Nodal Officer in the paragraphs 4.2 to 4.6 above. The Registrar should also ensure 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 State Nodal Officer, without delay.

(iii) The State Nodal Officer 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 or if any assets of such designated individual/ entity are with the Casino operator, or if the particulars of any client match with the particulars of designated individuals/ entities, the Casino owner shall inform the State Nodal Officer, without delay, and shall freeze any such transaction.

(iv) 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 12A, 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 Section 12A Nodal Officer in the Ministry of Corporate Affairs, who shall in turn follow the similar procedure as laid down for State Nodal Officer in paragraph 4.2 to 4.6 above.

(v) The members of these institutes should also be sensitized by the Institute of Chartered Accountants of India, Institute of Cost and Work Accountants of India and Institute of Company Secretaries of India (ICSI) 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 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 Section 12A Nodal Officer in the Ministry of Corporate Affairs.

(vi) In addition, a member of the ICSI shall, 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, convey the complete details of such designated individual/ entity to Section 12A Nodal Officer in the Ministry of Corporate Affairs, who shall follow the similar procedure as laid down in paragraph 4.2 to 4.6 above for State Nodal Officer, if such company, limited liability firm, partnership firm, society, trust, or association holds funds or assets of the designated individual/entity.

(vii) In case any designated individual/ entity is a shareholder/ director/ whole time director in any company registered with the Registrar of Companies (ROC) or beneficial owner of such company or partner in a Limited Liabilities Partnership Firm registered with ROC or beneficial owner of such firm, the ROC should convey the complete details of such designated individual/ entity to section 12A Nodal officer of Ministry of Corporate Affairs. If such company or LLP holds funds or assets of the designated individual/ entity, he shall follow the similar procedure as laid down in paragraph 4.2 to 4.6 above for State Nodal Officer. Further the ROCs are required to ensure 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 is received, the ROC should inform the Section 12A Nodal Officer in the Ministry of Corporate Affairs.

(viii) All communications to Nodal officer as enunciated in subclauses (i) to (vii) above should, inter alia, include the details of funds and assets held and the details of transaction.

(ix) The Other DNBPs are required to ensure that if any designated individual/entity approaches them for a transaction or relationship or attempts to undertake such transactions, the dealer should not carry out such transaction and, without delay, inform the Section 12A Central Nodal officer. The communication to the Central Nodal Officer would include the details of funds and assets held and the details of the transaction. Also, If the dealers hold any assets or funds of the designated individual/entity, they shall freeze the same without delay and inform the Section 12A Central Nodal officer.

(DNFBPs shall have the same meaning as the definition in Section 2(1) (sa) of Prevention of Money-Laundering Act, 2002.)

5.1. All Natural and legal persons holding any funds or other assets of designated persons and entities, shall, without delay and without prior notice, freeze any transaction in relation to such funds or assets and shall immediately inform the State Nodal officer along with details of the funds/assets held, who in turn would follow the same procedure as in para 4.2 to 4.6 above for State Nodal Officer. This obligation should extend to all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation; those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

5.2 No person shall finance any activity related to the 'designated list' referred to in Para 2.1, except in cases where exemption has been granted as per Para 6 of this Order.

5.3. Further, the State Nodal Officer 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 in the designated list. The State Nodal Officer shall, upon becoming aware of any transactions and attempts by third party, without delay, bring the incidence to the notice of the CNO and the DGP/Commissioner of Police of the State/UT for initiating suitable action.

5.4 Where the CNO has reasons to believe that any funds or assets are violative of Section 12A (1) or Section 12A (2)(b) of the Act, he shall, by order, freeze such funds or Assets, without any delay, and make such order available to authorities, Financial Institutions, DNFBPs and other entities concerned.

5.5 The CNO shall also have the power to issue advisories and guidance to all persons, including Fls and DNFBPs obligated to carry out sanctions screening. The concerned Regulators shall take suitable action under their relevant laws, rules or regulations for each violation of sanction screening obligations under section 12A of the WMD Act.

6. Regarding exemption, to be granted to the above orders

6.1. The above provisions shall not apply to funds and other financial assets or economic resources that have been determined by the CNO 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, consequent to notification by the MEA authorizing access to such funds, assets or resources.

This shall be consequent to notification by the MEA to the UNSC or its Committee, of the intention to authorize access to such funds, assets or resources, and in the absence of a negative decision by the UNSC or its Committee within 5 working days of such notification.

(b) necessary for extraordinary expenses, provided that such determination has been notified by the MEA to the UNSC or its Committee, and has been approved by the UNSC or its Committee;

6.2. The accounts of the designated individuals/ entities may be allowed to be credited with:

(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 section 12A of the Act.

Provided that any such interest, other earnings and payments continue to be subject to those provisions under para 3.3;

6.3 Any freezing action taken related to the designated list under this Order should not prevent a designated individual or entity from making any payment due under a contract entered into prior to the listing of such individual or entity, provided that:

(i) the CNO has determined that the contract is not related to any of the prohibited goods, services, technologies, or activities, under this Act, or under the United Nations (Security Council) Act, 1947 or any other relevant Act for the time being in force, or by an order issued under any such Act, in relation to weapons of mass destruction and their delivery systems;

(ii) the CNO has determined that the payment is not directly or indirectly received by an individual or entity in the designated list under this Order; and

(iii) the MEA has submitted prior notification to the UNSC or its Committee, of the intention to make or receive such payments or to authorise, where appropriate, he unfreezing of funds, other financial assets or economic resources for this purpose, ten working days prior to such authorization

7. 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 individual or entity is not a designated person or no longer meet the criteria for designation:

7.1 Any individual/entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held has been inadvertently frozen, an application may be moved giving the requisite evidence, in writing, to the relevant RE/Registrar of Immovable Properties/ ROC/Regulators and the State.

7.2 The RE/Registrar of Immovable Properties/ROC/Regulator and the State Nodal Officer shall inform, and forward a copy of the application, together with full details of the asset frozen, as given by applicant to the CNO by email, FAX and by Post, within two working days. Also, listed persons and

entities may petition a request for delisting at the Focal Point Mechanism established under UNSC Resolution.

7.3 The CNO shall cause such verification, as may be required on the basis of the evidence furnished by the individual/entity, and, if satisfied, it 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 all RE/Registrar of Immovable Properties/ROC/Regulators and the State Nodal Officer. However, if it is not possible, for any reason, to pass an Order unfreezing the assets within 5 working days, the CNO shall inform the applicant expeditiously.

7.4 The CNO shall, based on de-listing of individual and entity under UN Security Council Resolutions, shall pass an order, if not required to be designated in any other order, without delay, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant, under intimation to all RE/Registrar of Immovable Properties/ROC/Regulators and the State Nodal Officer.

8. Procedure for communication of compliance of action taken under Section 12A: The CNO 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.

9. Communication of the Order issued under Section 12A: The Order issued under Section 12A of the Act by the CNO relating to funds, financial assets or economic resources or related services, shall be communicated to all nodal officers in the country.

10. This order is issued in suppression of F.No.P-12011/14/2022-ES Cell-DOR, dated 30th January 2023.

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

(Manoj Kumar Singh)
Director (HQ)

To,
1) Governor, Reserve Bank of India, Mumbai
2) Chairman, Securities & Exchange Board of India, Mumbai
3) Chairman, Insurance Regulatory and Development Authority, Hyderabad.
4) Foreign Secretary, Ministry of External Affairs, New Delhi.
5) Finance Secretary, Ministry of Finance, New Delhi.
6) Revenue Secretary, Department of Revenue, Ministry of Finance, New Delhi.
7) Secretary, Ministry of Corporate Affairs, New Delhi
8) Chairman, Central Board of Indirect Taxes & Customs, New Delhi.
9) Director, Intelligence Bureau, New Delhi.
10) Additional Secretary, Department of Financial Services, Ministry of Finance, New Delhi.

11) Chief Secretaries of all States/Union Territories
12) Principal Secretary (Home)/Secretary (Home) of all States/ Union Territories
13) Directors General of Police of all States & Union Territories
14) Director General of Police, National Investigation Agency, New Delhi.
15) Commissioner of Police, Delhi.
16) Joint Secretary (Foreigners), Ministry of Home Affairs, New Delhi.
17) Joint Secretary (Capital Markets), Department of Economic Affairs, Ministry of Finance, New Delhi.
18) Joint Secretary (Revenue), Department of Revenue, Ministry of Finance, New Delhi.
19) Director (FIU-IND), New Delhi.

Copy for information to: -
1. Sr. PPS to HS
2. PS to SS (IS)

ANNEXURE- VI

KYC documents for eligible Foreign Portfolio Investors under Portfolio Investment Scheme.

		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, **Asset Reconstruction Companies (ARCs)** 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.

LIST OF COUNTRIES WITH RISK CLASSIFICATION — Annexure-VII

The list of Countries with risk classification											
SR No	COUNTRY	Country Risk Classification	SR No	COUNTRY	Country Risk Classification	SR No	COUNTRY	Country Risk Classification	SR No	COUNTRY	Country Risk Classification
1	Afghanistan	HIGH	1	Albania	MEDIUM	51	Gabon	MEDIUM	101	North Macedonia	MEDIUM
2	Bahamas	HIGH	2	Algeria	MEDIUM	52	Gambia	MEDIUM	102	Norway	MEDIUM
3	Barbados	HIGH	3	Andorra	MEDIUM	53	Georgia	MEDIUM	103	Oman	MEDIUM
4	Botswana	HIGH	4	Angola	MEDIUM	54	Grenada	MEDIUM	104	Palau	MEDIUM
5	Cambodia	HIGH	5	Antigua&Barbuda	MEDIUM	55	Guatemala	MEDIUM	105	Palestine State	MEDIUM
6	Ghana	HIGH	6	Argentina	MEDIUM	56	Guinea	MEDIUM	106	Papua New Guinea	MEDIUM
7	Iran	HIGH	7	Armenia	MEDIUM	57	Guinea-Bissau	MEDIUM	107	Paraguay	MEDIUM
8	Iraq	HIGH	8	Azerbaijan	MEDIUM	58	Guyana	MEDIUM	108	Peru	MEDIUM
9	Jamaica	HIGH	9	Bahrain	MEDIUM	59	Haiti	MEDIUM	109	Philippines	MEDIUM
10	Mauritius	HIGH	10	Bangladesh	MEDIUM	60	Holy See	MEDIUM	110	Qatar	MEDIUM
11	Mongolia	HIGH	11	Belarus	MEDIUM	61	Honduras	MEDIUM	111	Rwanda	MEDIUM
12	Myanmar (formerly Burma)	HIGH	12	Belgium	MEDIUM	62	Iceland	MEDIUM	112	Saint Kitts&Nevis	MEDIUM
13	Nicaragua	HIGH	13	Belize	MEDIUM	63	Indonesia	MEDIUM	113	Saint Lucia	MEDIUM
14	North Korea	HIGH	14	Benin	MEDIUM	64	Ireland	MEDIUM	114	Saint Vincent and the Grenadines	MEDIUM
15	Pakistan	HIGH	15	Bhutan	MEDIUM	65	Israel	MEDIUM	115	Samoa	MEDIUM
16	Panama	HIGH	16	Bolivia	MEDIUM	66	Jordan	MEDIUM	116	San Marino	MEDIUM
17	Syria	HIGH	17	Bosnia& Herzegovina	MEDIUM	67	Kazakhstan	MEDIUM	117	Sao Tome and Principe	MEDIUM
18	Trinidad and Tobago	HIGH	18	Brazil	MEDIUM	68	Kenya	MEDIUM	118	Saudi Arabia	MEDIUM
19	Uganda	HIGH	19	Brunei	MEDIUM	69	Kiribati	MEDIUM	119	Senegal	MEDIUM
20	Vanuatu	HIGH	20	Bulgaria	MEDIUM	70	Kuwait	MEDIUM	120	Serbia	MEDIUM
21	Yemen	HIGH	21	Burkina Faso	MEDIUM	71	Kyrgyzstan	MEDIUM	121	Seychelles	MEDIUM
22	Zimbabwe	HIGH	22	Burundi	MEDIUM	72	Laos	MEDIUM	122	Sierra Leone	MEDIUM
23	**Gibraltar**	**HIGH**	23	Côte d'Ivoire	MEDIUM	73	Latvia	MEDIUM	123	Slovakia	MEDIUM
24	**Guernsey**	**HIGH**	24	Cabo Verde	MEDIUM	74	Lebanon	MEDIUM	124	Slovenia	MEDIUM
25	**Jersey**	**HIGH**	25	Cameroon	MEDIUM	75	Lesotho	MEDIUM	125	Solomon Islands	MEDIUM
26	**Korea, Democratic**	**HIGH**	26	Central African	MEDIUM	76	Liberia	MEDIUM	126	Somalia	MEDIUM
			27	Chad	MEDIUM	77	Libya	MEDIUM	127	South Africa	MEDIUM
			28	Chile	MEDIUM	78	Liechtenstein	MEDIUM	128	South Sudan	MEDIUM
			29	China	MEDIUM	79	Lithuania	MEDIUM	129	Sri Lanka	MEDIUM
			30	Colombia	MEDIUM	80	Madagascar	MEDIUM	130	Sudan	MEDIUM
			31	Comoros	MEDIUM	81	Malawi	MEDIUM	131	Suriname	MEDIUM
			32	Congo (Congo-Brazzaville)	MEDIUM	82	Malaysia	MEDIUM	132	Tajikistan	MEDIUM
			33	Costa Rica	MEDIUM	83	Maldives	MEDIUM	133	Tanzania	MEDIUM
			34	Croatia	MEDIUM	84	Mali	MEDIUM	134	Thailand	MEDIUM
			35	Cuba	MEDIUM	85	Malta	MEDIUM	135	Timor-Leste	MEDIUM
			36	Cyprus	MEDIUM	86	Marshall Island	MEDIUM	136	Togo	MEDIUM
			37	Czechia (Czech Republic)	MEDIUM	87	Mauritania	MEDIUM	137	Tonga	MEDIUM
			38	Democratic Republic of the Congo	MEDIUM	88	Mexico	MEDIUM	138	Tunisia	MEDIUM
			39	Djibouti	MEDIUM	89	Micronesia	MEDIUM	139	Turkey	MEDIUM
			40	Dominica	MEDIUM	90	Moldova	MEDIUM	140	Turkmenista	MEDIUM
			41	Dominican Republic	MEDIUM	91	Monaco	MEDIUM	141	Tuvalu	MEDIUM
			42	Ecuador	MEDIUM	92	Montenegro	MEDIUM	142	Ukraine	MEDIUM
			43	Egypt	MEDIUM	93	Morocco	MEDIUM	143	United Arab Emirates	MEDIUM
			44	El Salvador	MEDIUM	94	Mozambique	MEDIUM	144	Uruguay	MEDIUM
			45	Equatorial Guinea	MEDIUM	95	Namibia	MEDIUM	145	Uzbekistan	MEDIUM
			46	Eritrea	MEDIUM	96	Nauru	MEDIUM	146	Venezuela	MEDIUM
			47	Estonia	MEDIUM	97	Nepal	MEDIUM	147	Vietnam	MEDIUM
			48	Eswatini ("Swaziland")	MEDIUM	98	Netherlands	MEDIUM	148	Zambia	MEDIUM
			49	Ethiopia	MEDIUM	99	Niger	MEDIUM	**149**	**Aruba**	**MEDIUM**
			50	Fiji	MEDIUM	100	Nigeria	MEDIUM			

List of countries with Risk classification

SR No	COUNTRY	Country Risk Classification	SR No	COUNTRY	Country Risk Classification
1	Australia	LOW	39	Falkland Islands (Malvinas)	LOW
2	Austria	LOW	40	Faroe Islands	LOW
3	Canada	LOW	41	French Guiana	LOW
4	Denmark	LOW	42	French Polynesia	LOW
5	Finland	LOW	43	French Southern Territories	LOW
6	France	LOW	44	Greenland	LOW
7	Germany	LOW	45	Guadeloupe	LOW
8	Greece	LOW	46	Guam	LOW
9	Hungary	LOW	47	Heard Island and McDonald Islands	LOW
10	Italy	LOW	48	Hong Kong	LOW
11	Japan	LOW	49	Isle of Man	LOW
12	Luxembourg	LOW	50	Korea, Republic of	LOW
13	New Zealand	LOW	51	Macao	LOW
14	Poland	LOW	52	Macedonia, the former Yugoslav Republic of	LOW
15	Portugal	LOW	53	Martinique	LOW
16	Romania	LOW	54	Mayotte	LOW
17	Russia	LOW	55	Montserrat	LOW
18	Singapore	LOW	56	New Caledonia	LOW
19	South Korea	LOW	57	Niue	LOW
20	Spain	LOW	58	Norfolk Island	LOW
21	Sweden	LOW	59	Northern Mariana Islands	LOW
22	Switzerland	LOW	60	Pitcairn	LOW
23	United Kingdom	LOW	61	Puerto Rico	LOW
24	United States of America	LOW	62	Reunion !Réunion	LOW
25	Aland Islands	LOW	63	Saint Barthelemy !Saint Barthélemy	LOW
26	American Samoa/OPTION>	LOW	64	Saint Helena, Ascension and Tristan da Cunha	LOW
27	Anguilla	LOW	65	Saint Pierre and Miquelon	LOW
28	Antarctica	LOW	66	Saint Vincent and the Grenadines	LOW
29	Bermuda	LOW	67	Sint Maarten (Dutch part)	LOW
30	Bonaire, Sint Eustatius and Saba	LOW	68	Svalbard and Jan Mayen	LOW
31	Bouvet Island	LOW	69	Swaziland	LOW
32	British Indian Ocean Territory	LOW	70	Taiwan, Province of China	LOW
33	Christmas Island	LOW	71	Tokelau	LOW
34	Cocos (Keeling) Islands	LOW	72	Turks and Caicos Islands	LOW
35	Congo, the Democratic Republic of the	LOW	73	United States Minor Outlying Islands	LOW
36	Cook Islands	LOW	74	Virgin Islands, British	LOW
37	Cote d'Ivoire !Côte d'Ivoire	LOW	75	Virgin Islands, U.S.	LOW
38	Curacao !Curaçao	LOW	76	Wallis and Futuna	LOW

Annexure-VIII

FREQUENTLY ASKED QUESTIONS (FAQs)

Q 1. What is KYC?

Response: KYC is an acronym for ―Know your Customer, a term used for Customer identification process. It is a process by which banks obtain information about the identity and address of the customers 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.

It involves making reasonable efforts to determine, the true identity and beneficial ownership of accounts, source of funds, financial status & nature of customer‘s business, reasonableness of operations in the account in relation to the customer‘s overall profile, etc. which in turn helps the banks to manage their risks prudently.

Q 2. What is the objective of KYC?

Response: The objective of the KYC guidelines is to prevent Bank from being used, intentionally or unintentionally, by criminal elements for Money Laundering or Terrorist Financing activities.

KYC procedures also enable the Bank to know/understand their customers and their financial dealings better, which in turn helps it to manage the associated risks prudently and enable the Bank to comply with all the legal and regulatory obligations in respect of KYC norms / AML standards / CFT measures / Bank‘s Obligation under PMLA, 2002 and to cooperate with various government bodies dealing with related issues.

Q 3. What is Money Laundering and Terrorist financing?

Response: Money laundering refers to conversion of money illegally obtained to make it appear as if it originated from a legitimate source. Money laundering is being employed by launderers worldwide to conceal criminal activity associated with it such as drugs /arms trafficking, terrorism and extortion. Terrorist financing means financial support to, in any form of terrorism or to those who encourage, plan or engage in terrorism. Money launderers send illicit funds through legal channels in order to conceal their criminal origin while those who finance terrorism transfer funds that may be legal or illicit in original in such a way as to conceal their source and ultimate use, which is to support Terrorist financing.

Money laundering has become a pertinent problem worldwide threatening the stability of various regions by actively supporting and strengthening terrorist networks and criminal organizations. The links between money laundering, organized crime, drug trafficking and terrorism pose a risk to financial institutions globally. Government of India has promulgated Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, and RBI Master Direction on KYC, enforces legal/statutory/regulatory obligations on both bank and customers to provide KYC information/documents.

Q 4. Whether KYC is mandatory?

Response: Yes. It‘s a regulatory and legal requirement. Regulatory: - In terms of the guidelines issued by the Reserve Bank of India (RBI) on 29 November, 2004 on Know Your Customer (KYC)

Standards - Anti Money Laundering (AML) measures, all banks are required to put in place a comprehensive policy framework covering KYC Standards and AML Measures. Legal:- The Prevention of Money Laundering Act, 2002 (PMLA) which came into force from 1st July, 2005 (after ―rules‖ under the Act were formulated and published in the Official Gazette) also requires Banks, Financial Institutions and Intermediaries to ensure that they follow certain minimum standard of KYC and AML as laid down in the ACT and the ―rules‖ framed thereunder.

Q 5. Is KYC information obtained from customer kept confidential?

Response: Yes, the customer profile/information collected by the Bank at the time, of account opening or otherwise, are kept confidential and are not disclosed to any person, except when required under the provisions of applicable laws and regulations or where there is a duty to the public to disclose or the interest of bank requires disclosure.

Q 6. What are the documents to be obtained from customers as 'proof of identity' and 'proof of address'?

Response: The Government of India has notified six documents or its equivalent e-documents as 'Officially Valid Documents (OVDs) for the purpose of producing proof of identity of individual customers. These six documents are the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address**.**

You need to submit any one of these documents as proof of identity. If these documents also contain your current address details, then it would be accepted as 'proof of address'. Provided that if customer is desirous of receiving any benefit or subsidy under any scheme notified under Aadhaar Act, 2016, customer shall be required to undertake Aadhaar authentication using e-KYC facility of UIDAI.

KYC documents to be obtained from non-individual customers have been specified in the KYC policy.

Q 7. If customer do not have any of the OVDs listed above with current updated address, can customer provide other OVD?

Response: Yes, customer can provide the following documents or the equivalent e-documents for the limited purpose of proof of address, with an undertaking along with AOF/OVDs stating that he/she shall submit his OVD with updated current address within 3 months failing which operations in his/her account shall be restricted.

- Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
- Property or Municipal tax receipt;
- Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

- Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and
- Leave and license agreements with such employers allotting official accommodation.

However, if customer undertakes Aadhaar authentication using e-KYC facility of UIDAI and 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.
70 Know Your Customer (KYC) Policy, 2020 Version: 2020_KYC_1.0

Q 8. Are there any additional documents to be obtained from customer apart from 'proof of identity' and 'proof of address'?

Response: Yes, at least one document in support of the declared Profession / activity, nature of business, financial status, annual income/ turnover (in case of business) has to obtained from individual customers; such as Salary Slip, Registration certificate, Certificate / license issued by the municipal authorities under Shop and Establishment Act, Sales and income tax returns, CST / VAT / GST certificates, Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, License / certificate of practice issued by any professional body incorporated under a statue, Complete Income Tax Returns (Not just the acknowledgement) etc.

Q 9. What if the customer doesn't have any document in support of nature of business, financial status, annual income?

Response: Customers who don't have any business / financial activity or don't have any proof in this regard such as housewife, student, minor, labour working in un-organized sector, farmers etc may submit self-declaration to this effect.

Q 10. If customer does not have any of the documents listed above to show his/her 'proof of identity', can he/she still open a bank account?

Response: Yes, customer can still open a bank account known as 'Small Account', which entails certain limitations, by submitting his/her recent photograph and putting signature or thumb impression in the presence of a bank official.

Q 11. Is there any difference between such 'small accounts' and other accounts?

Response: Yes. The 'Small Accounts' have certain limitations such as: balance in such accounts at any point of time should not exceed ₹50,000 total credits in one financial year should not exceed ₹1,00,000 total withdrawal and transfers should not exceed ₹10,000 in a month. Foreign remittances cannot be credited to such accounts. Such accounts remain operational initially for a period of twelve months and thereafter, for a further period of twelve months, if the holder of such an account provides evidence to the bank of having applied for any of the officially valid documents within twelve months of the opening of such account. The bank will review such account after twenty four months to see if it requires such relaxation.

Q 12. If customer refuses to provide requested documents for KYC to the bank for opening an account, what may be the result?
Response: If customer does not provide the required documents for KYC, the bank shall not open the account.

Q 13. Can a customer open bank account with only an Aadhaar card?

Response: As per RBI directions, Aadhaar card is now accepted as a proof of both, identity and address. However, PAN/Form 60 along with one document or the equivalent e-document thereof in support of the declared Profession / activity, nature of business or financial status is also required.

Q 14. Is Aadhaar mandatory for opening of an account?

Response: No, Aadhaar is not mandatory for opening of an account. As per RBI directions, only an individual who is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016) is mandatorily required to provide Aadhaar and is required to undertake Aadhaar authentication using e-KYC facility of UIDAI.

Q 15. What is e-KYC? How does e-KYC work?

Response: e-KYC refers to electronic KYC. e-KYC is possible only for those who have Aadhaar number or proof of possession of Aadhaar. While using e-KYC service, customer has to authorize the Unique Identification Authority of India (UIDAI), by explicit consent, to release his/her identity/address through biometric authentication to the bank branches/business correspondent (BC). The UIDAI then transfers his/her data comprising name, age, gender, and photograph of the individual, electronically to the bank/BC. Information thus provided through e-KYC process is permitted to be treated as an 'Officially Valid Document' under PML Rules and is a valid process for KYC verification.

Q 16. Is introduction necessary while opening a bank account?

Response: No, introduction is not required.

Q 17. Can a customer transfer his existing bank account from one branch to another?

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

Q 18. Is a customer required to furnish KYC documents for each account he/she opens in the Bank?

Response: As per RBI guidelines, an individual customer can maintain only a single Unique Customer ID Code (UCIC)/Customer-ID in a Bank and all the accounts of the customer have to be opened/ linked under this Customer-ID. Therefore, if a customer has opened an account with the Bank, which is KYC compliant, then for opening another account, furnishing of documents is not necessary.

Q 19. Customer's KYC was completed when he/she opened the account. Why does Bank ask for doing KYC again?

Response: In terms of RBI guidelines, Bank is required to periodically update KYC records. This is a part of ongoing due diligence on bank accounts. The periodicity of such updation varies from account to account or categories of accounts depending on the Bank's perception of risk. Further, the Bank may insist for KYC updation, whenever there is a doubt about the authenticity or adequacy of the customer identification data it has obtained. Regular monitoring of transactions in accounts is required to ensure that **those** are consistent with **Bank's knowledge about the customers, customers' business and risk profile, the source of funds / wealth**.

Q 20. What are the rules regarding periodical updation of KYC?

Response: Different periodicities have been prescribed for updation of KYC records depending on the risk perception of the bank. Periodic updation of KYC is to 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. Branch has to review the documents sought at the time of opening of account and obtain fresh certified copies from customer. However, 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 may be obtained.
Provided Branch has to ensure that KYC documents, as per extant requirements of the Master Direction, are available with the Bank.

Q 21. What if the customer does not provide KYC documents at the time of periodic updation?

Response: If customer does not provide his/her KYC documents at the time of periodic updation, Bank shall temporarily cease operations in the account. The account holders shall have the option to revive their accounts by submitting the KYC documents.

Q 22.Do the customer need to submit KYC documents to the bank while purchasing third party products (like insurance or mutual fund products) from banks?

Response: Yes, all customers who do not have accounts with the Bank (known as walk-in customers) have to produce proof of identity and address while purchasing third party products from Bank if the transaction is for ₹50,000 and above. KYC exercise may not be necessary for bank's own customers for purchasing third party products. However, instructions to make payment by debit to customers' accounts or against cheques for remittance of funds/issue of travellers' cheques, sale of gold/silver/platinum and the requirement of quoting PAN number for transactions of ₹50,000 and above would be applicable to purchase of third party products from Bank by Bank's customers as also to walk-in customers.

Q 23. Whether the Customer Due Diligence (CDD) of all the members of the Self Help Group is required at the time of credit linking of SHGs?

Response: Yes, Customer Due Diligence (CDD) of all the members of SHG should be undertaken at the time of credit linking of SHGs, however, for opening of savings Bank account of SHGs, KYC verification / Customer due diligence of all office bearers will be sufficient.