KYC-AML-CFT POLICY-2023-24

Updated as on 20.05.2023

1. Introduction

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

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

RBI has advised banks to put in place a policy on 'Know Your Customer' and 'Anti-Money Laundering' measures including the above referred recommendations with the approval of the Board and shall take steps to implement the provisions of the aforementioned Act and Rules, issued in **pursuance** of such amendment(s).

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

This policy has been compiled covering the guidelines issued by RBI/GOI up to 4 May 2023.

2. Objective

2.1 To lay down policy framework for abiding by the Know Your Customer Norms and Anti-Money Laundering Measure as set out by Reserve Bank of India, based on the recommendations of the Financial Action Task Force (FATF) and the paper issued on Customer Due Diligence (CDD) for banks issued by the Basel Committee on Banking Supervision.

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

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

2.4 Bank shall ensure that a group-wide policy is implemented for the purpose of discharging obligations under the provisions of Chapter IV of the Prevention of Money-laundering Act, 2002 (15 of 2003).

2.5 Bank's 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.

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

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

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

3. Scope

This policy is applicable across all Branches/offices of the Bank and is to be read in conjunction with related operational guidelines issued from time to time.

The contents of the policy shall be subject to the changes / modifications which may be advised by RBI and / or by any regulators and / or by Bank from time to time

4. Definitions

1. Aadhaar Number

"Aadhaar number" means an identification number issued to an individual by submitting the demographic information such as Name, Date of birth (verified) or age (declared), Gender, Address, Mobile Number (optional), email ID (optional) and biometric information such as Ten Fingerprints, Two Iris Scans and Facial Photograph. It is 12-digit random number issued by Unique Identification Authority of India (UIDAI)

2. Act and Rules

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

3. Authentication

"Authentication", in the context of Aadhaar authentication, means the process by which the Aadhaar number along with the demographic information or biometric information of Aadhaar number holder is submitted to the Central Identities Data Repository (CIDR) for its verification.

4. Beneficial Owner (BO)

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

Explanation- For the purpose of this sub-clause-

i) "Controlling ownership interest" means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.

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

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

c) Where the **customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent of the property or capital or profits of the unincorporated association or body of individuals.
Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d) Where the customer is a **trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10 percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

5. Certified Copy

"Certified Copy" – Obtaining a certified copy by the branch 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.

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

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 non-resident customer resides.

6. Central KYC Records Registry (CKYCR)

"Central KYC Records Registry" is a reporting entity which is owned, controlled and authorized by the Central Government through official notification in the official gazette to safeguard the KYC records in the digital form and perform such functions as may be required. It includes receiving, storing and retrieving the KYC records of the clients.

7. Correspondent Banking

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Respondent banks may be provided with a wide range of services, including cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.

8. Customer

For the purpose of KYC Norms, a "Customer" is defined as a person who is engaged in a financial transaction or activity with the Bank and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

9. Customer Due Diligence (CDD)

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

10. Designated Director

"Designated Director" means a person designated by the Bank to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules. Bank has appointed Executive Director of Bank as Designated Director.

11. Digital KYC

"Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorized officer of the branch. The detailed process of digital KYC is explained in **ANNEXURE I.**

12. Digital Signature

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time stamped. A digital signature can be used with any kind of message, whether it is encrypted or plaintext.

"Digital Signature" authenticate any electronic record by a sender by means of an electronic method or procedure subject to the provisions:

a) Any sender may authenticate an electronic record by affixing his digital signature

b) The authentication of electronic record shall be effected by the use of asymmetric crypto system and hash function which develop and transform the initial electronic record into another electronic record.

Explanation: "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record

yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible:

i) To derive or reconstruct the original electronic record from the hash result produced by the algorithm;

ii) That two electronic records can produce the same hash result using the algorithm.

c) Any person by the use of a public key of the sender can verify the electronic record.

d) The private key and the public key are unique to the sender and constitute a functioning key pair.

13. Enhanced Due Diligence (EDD)

Any additional due diligence measures undertaken over and above the standard level of due diligence is termed as Enhanced Due Diligence. EDD can be applied at the product level or customer type level where the suspicion of money laundering or terrorist financing is high. Some of the parameters which can be used for enhanced due diligence are:

a) Customer location
b) Nature of business /occupation;
c) Transactions in line with the business activity / occupation;
d) Number and value of transaction;
e) Public domain checks for adverse media news on customer

Indicative examples of what can constitute Enhanced Due Diligence

I. Obtaining additional identifying information from a wider variety or more robust sources and using the information to inform the individual customer risk assessment.
II. Carrying out additional searches (e.g., verifiable adverse media searches) to inform the individual customer risk assessment.
III. Verifying the source of funds or wealth involved in the business relationship to be satisfied that they do not constitute the proceeds from crime.

Seeking additional information from the customer about the purpose and intended nature of the business relationship.

14. Equivalent e-document

“Equivalent e-document” means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016. Equivalent e-document has also been permitted for accounts of non-individual customers.

15. Group

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

16. Know Your Customer (KYC) Identifier

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

17. Non face to face customer

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

18. Non-profit Organisations (NPO)

A 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 At, 1961 (43 of 1961), that is registered as a Trust or a Society under the Societies Registration Act, 1860 (21 of 1860) or any similar State Legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013)

19. Officially valid Document (OVD)

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

Provided that,

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

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

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

ii. Property or Municipal tax receipt;

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

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

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

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

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

20. Offline Verification

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

Offline verification is defined as a process of verifying the identity of an individual through offline modes. The modes for offline verification have not been specified and left upon Unique Identification Authority of India (UIDAI) to specify, by means of regulations.

During offline verification, the branches / bank must:

a) Obtain the consent of the individual,
b) Inform them of alternatives to sharing information, and
c) Not to collect, use or store Aadhaar number or biometric information.

21. On-going Due Diligence

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

22. Payable-through accounts

The term payable-through accounts refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

23. Periodic Updation

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

24. Person

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

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

25. Politically Exposed Persons (PEPs)

"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.

26. Principal Officer

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

27. 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.

28. Simplified Due Diligence (SDD)

Any due diligence applied to establish the identity of customer, which involves measures less stringent then basic due diligence can be termed as 'Simplified Due Diligence'. Obtaining less information or alternate information based on the particular type of customer & based on availability of documents and/or seeking less robust verification, of the customer's location identity and the purpose and intended nature of the business relationship.

29. Suspicious transaction

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

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

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

30. Transaction

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

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

c) The use of a safety deposit box or any other form of safe deposit;
d) Entering into any fiduciary relationship;
e) Any payment made or received, in whole or in part, for any contractual or other legal obligation

Establishing or creating a legal person or legal arrangement.

31. Video based Customer Identification Process (V-CIP)

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

32. Walk-in Customer

"Walk-in customer" means a person who does not have an account based relationship with the bank, but undertakes transaction with the bank.

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

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

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. Key Elements of the policy

KYC policy of the bank has following four key elements:

a. Customer Acceptance Policy,

b. Risk Management

c. Customer Identification Procedures and

d. Monitoring of Transactions.

5.1 Customer Acceptance Policy (CAP)

Bank shall develop clear Customer Acceptance Policies and procedures, including a description of the types of customers that are likely to pose a higher than average risk to the bank and including the following aspects of customer relationship in the Bank are:

i. No account is opened or maintained in anonymous or fictitious / benami name.

ii. **While opening an account and during the periodic updation**, documents and other information to be collected from different categories of customers are detailed in **ANNEXURE - II of this policy.**

iii. Bank will not open an account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and / or obtain required documents either due to non-cooperation of the customer or non-reliability of the documents / information furnished by the customer. Bank may also consider closing an existing account under similar circumstances.

iv. Additional information, where such information requirement has not been specified in the internal KYC Policy of the bank, is obtained with the explicit consent of the customer .

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

vi. Circumstances, in which a customer is permitted to act on behalf of another person / entity, shall be clearly spelt out in conformity with the established law and practice of banking.

vii. Bank shall have suitable systems in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanction lists circulated by the Reserve Bank.

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

ix. While opening joint account, CDD Procedure is followed for all the joint account holders.

x. Through digital signature branch shall verify an equivalent e-document which is obtained from the customer **as explained in 4.13 in this policy**.

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

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

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

Adoption of customer acceptance policy and its implementation shall not become too restrictive, which result in denial of banking facility to the members of the general public, especially to those, who are financially or socially disadvantaged.

5.1.1 Unique Customer Identification number (UCIC)

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

In our Bank, CIF of the customer is the Unique Number for that customer, and it serves the purpose of Unique Customer Identification Code (UCIC).

Before creating a new CIF for any customer for opening any new account, branch should first verify that the same customer has not an existing CIF in the CBS system. If a customer has already been allotted a CIF, the new account(s) of that customer must be opened under the existing CIF only. No additional CIF should be created for him/her. For finding out the existing CIFs of all existing customers, "CIF Search" utility is provided under Intranet (ULC) to the branches, which must be used before opening any new account for any customer.

Utility for knowing the customers already having multiple CIFs in the system is also provided to the branches. Branches should check up the reports provided under this utility on daily basis and undertake the exercise of keeping only one CIF for one customer by linking of additional CIFs created in the system for the same customer to a single CIF and deactivating all other CIFs.

A Unique Customer Identification Code (UCIC) will help the Bank to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable the Bank to have a better approach to risk profiling of customers. Branches are required to strictly avoid creating multiple customer IDs while opening new accounts and in case of existing multiple IDs, branches have to carry out the process of de-duplication.

The bank shall not issue UCIC to all walk-in / occasional customers such as buyers of prepaid instruments / purchasers of third-party products. However, UCIC shall be allotted to such walk-in customers who have frequent transactions in branch.

5.2 Customer Acceptance Policy (CAP)

The inadequacy or absence of KYC standards can subject the Bank to serious customer and counter party risks especially reputational, operational, legal and concentration risks.

5.2.1 Reputational Risk

Reputational Risk is defined as "the potential that adverse publicity regarding the Bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution".

5.2.2 Operational Risk

It can be defined as "the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events."

5.2.3 Legal Risk

Legal Risk is "the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of the Bank".

5.2.4 Concentration Risk

Concentration risk although mostly applicable on the assets side of the balance sheet, may affect the liabilities side as it is also closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the Bank's liquidity.

5.2.5 Risk perception in respect of customer

It is worth noting that all these risks are interrelated. Any one of them can result in significant financial cost to the Bank as well as the need to divert considerable management time and energy to resolve problems that arise.

Customers frequently have multiple accounts with the Bank, but in offices located at different places. To effectively manage the reputational, operational and legal risk arising from such accounts, Bank shall aggregate and monitor significant balances and activity in these accounts on a fully consolidated basis, whether the accounts are held as on balance sheet, off balance sheet or as assets under management or on a fiduciary basis.

Branches should exercise ongoing due diligence with respect to the business relationship with every customer and closely examine the transactions in order to ensure that they are consistent with their knowledge about the clients, their business and risk profile and where necessary, the source of funds. The Board of Directors of the Bank shall ensure that an effective KYC/AML/CFT programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It shall cover proper management oversight, systems and controls, segregation of duties, training of staff and other related matters. In addition, the following also to be ensured for effectively implementing the AML/CFT requirements:

i. Using a risk-based approach to address management and mitigation of various AML/CFT risks.
ii. Allocation of responsibility for effective implementation of policies and procedures.
iii. Independent evaluation by the compliance functions of Bank's policies and procedures, including legal and regulatory requirements.
iv. Concurrent/internal audit/snap audit to verify the compliance with KYC/AML policies and procedures.

v. Putting up consolidated note on such audits and compliance to the Audit Committee Board (ACB) at quarterly intervals and to Board of Directors as and when specified by Inspection & Audit Department.

Branches shall prepare a profile for each new customer based on risk categorization. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the Bank. Branches shall categorise the customers into low, medium and high risk category based on the assessment and risk perception of the customers, identifying transactions that fall outside the regular pattern of activity and not merely based on any group or class they belong to. The Bank shall have a Board approved policy for risk categorisation and ensure that the same is meticulously complied with, to effectively help in combating money laundering activities. The nature and extent of due diligence, shall be based on the following principles:

i. Individuals (other than High Net Worth) and entities, whose identity and source of income, can be easily identified, and customers in whose accounts the transactions conform to the known profile, shall be categorised as low risk. Illustrative examples include salaried employees and pensioners, people belonging to lower economic strata, government departments and government owned companies, regulators and statutory bodies, etc.

ii. Customers who are likely to pose a higher than average risk shall be categorized as medium or high risk depending on the background, nature and location of activity, country of origin, sources of funds, customer profile, etc. Customers requiring very high level of monitoring, e.g., those involved in cash intensive business, Politically Exposed Persons (PEPs) of foreign origin, shall be categorised as high risk.

iii. Whenever there are suspicions of money laundering or financing of activities relating to terrorism or where there are doubts about the veracity of previously obtained customer identification data, branches should review the due diligence measures including verifying again the identity of the customer and obtaining information on the purpose and intended nature of business relationship.

iv. Bank has adopted a risk categorization model as advised by the Indian Banks Association.

'Customer risk' in the present context refers to the money laundering and terrorist funding risk associated with a particular customer from a bank's perspective. This risk is based on risk perceptions associated with customer profile and level of risk associated with the product and channels used by the customer.

5.2.6 Customer Risk categorisation

For effective implementation of KYC, anti-money laundering (AML) and combating of financing of terrorism (CFT) measures, Risk categorizing a customer as Low Risk, Medium Risk and High Risk.

Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of

products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

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

i. Low Risk Customers

Individuals (other than High Net worth) and entities whose identities and sources of income can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorised as Low Risk customers, such as:

- Salaried employees
- People belonging to lower economic strata of the society
- Government Departments
- Government owned companies
- Regulatory and Statutory bodies, etc.

For the above category, the KYC requirements of proper identification and verification of proof of address would suffice.

Updating KYC of Low-Risk Customers: Every 10 years.

ii. Medium Risk Customers

Customers who are likely to pose a higher than average risk to the Bank should be categorized as medium or high risk.

For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his/her customer profile, etc. besides proper identification.

An indicative list Medium Risk Customers is as under:

- Gas Dealers
- Car / boat / plane dealers
- Electronics (wholesale)
- Travel agency,
- Telemarketers,
- Telecommunication service providers
- Pawnshops,
- Auctioneers,
- Restaurants, Retail shops, Movie theatres etc.
- Sole practitioners
- Notaries
- Accountants
- Blind

- Purdanashin

Updating KYC of Medium-Risk Customers: Every 8 years.

iii. High Risk Customers

For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his customer profile, etc. besides proper identification. Bank shall subject such accounts to enhanced monitoring on an ongoing basis.

- Trusts, charities, NGOs and organizations receiving donations.
- Companies having close family shareholding or beneficial ownership
- Firms with 'sleeping partners'.
- Accounts under Foreign Contribution Regulation Act.
- Politically Exposed Persons (PEPs).
- Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner.
- Those with dubious reputation as per public information available.
- Accounts of non-face-to-face customers.
- High Net worth Individuals*
- Non-Resident customers.
- Accounts of Cash intensive businesses such as accounts of bullion dealers (including sub-dealers) & jewelers.

Updating KYC of High-Risk Customers: Every 2 years.

iv. Parameters defining High Net worth Individuals (HNIs)

Customers with any of the following shall be treated as High Net worth Individuals;

- Average balance exceeding Rs. 25 lakhs in SB.
- Average Balance exceeding Rs. 50 lakhs in CA.
- Term deposits exceeding Rs. 50 lakhs in aggregate.
- Annual turnover exceeding Rs. 25 lakhs in the SB account, and exceeding Rs. 100 lakhs in the CA account.
- VIPs such as head of Village / Town / City, Top Executives of Companies etc.

For arriving at average balance in Savings and Current account, average balance during the immediately preceding last half financial year shall be considered.

For term deposits, aggregate term deposits of the customer at any point of time during the current financial year shall be considered.

Parameters for defining High Net worth Individuals Customers with any of the following:

- Average balance of Rs. 100 lakhs and above in all deposit accounts (SB+CA+TD).
- Enjoying Fund based limits/term loans exceeding Rs. 100 lakhs

The categorization of customers under risk perception is only illustrative and not exhaustive. The branches may categorize the customers according to the risk perceived by them while taking into account the above aspects.

Branches shall prepare a Risk profile of each customer and apply enhanced due diligence measures on High Risk customers. IBA has provided in indicative list of High / Medium Risk products, Services, Geographies, Locations, etc., for Risk Based Transactions Monitoring by Banks.

As per IBA Working Group guidelines, Bank may choose to carry out either manual classification or automatic classification or a combination of both. Similarly, for selecting parameters, Bank may select the parameters based on the available data. Once the parameters are finalized, Bank may choose the appropriate risk rating / scoring models by giving due weightage to each parameter.

Bank has adopted combination of manual and automatic classification. Based on the availability of data, bank shall finalize parameters which are available in the system and the same shall be reviewed half yearly basis. System shall assign provisional risk categorization based on the system provided parameters. Branches shall review the same and make suitable modification/revision, if need be, based on remaining indicators as covered in the policy.

Branches shall prepare a profile for all customers based on Risk categorizations. The customer profile may contain information relating to Customer's identity, social / financial status, nature of business activity, information about his clients business and their location etc. the nature and extent of due diligence will depend on the risk perceived by the bank. Risk categorization shall be done based on selected parameters and assigning suitable risk category.

5.2.7 Risk Parameters

The first step in process of risk categorization is selection of parameters, which would determine customer risk.

IBA Core Group on KYC and AML in its guidance note for Banks on KYC/AML/CFT obligation of Banks under PMLA 2002 has suggested following indicative parameters which can be used, to determine the profile and risk category of Customers:

i. Customer Constitution: Individual, Proprietorship, Partnership, Private Ltd. etc.
ii. Business Segment: Retail, Corporate etc.
iii. Country of residence / Nationality: Whether India or any overseas location / Indian or foreign national.
iv. Product Subscription: Salary account, NRI products etc.
v. Economic Profile: HNI, Public Ltd. Company etc.
vi. Account Status: Active, inoperative, dormant.
vii. Account Vintage: Less than six months old etc.
viii. Presence in regulatory negative / PEP / Defaulters / Fraudster lists.
ix. Suspicious Transaction Report (STR) filed for the customer.
x. AML alerts.

Other parameters like source of funds, occupation, purpose of account opening, nature of business, mode of operation, credit rating etc. can also be used in addition of the above parameters. Bank shall adopt all or majority of these parameters based on availability of data.

Periodical review of risk categorization of customers shall be undertaken once in every six months. Such review for the first half of the financial year i.e. April to September shall be undertaken in

succeeding November and for second half of the financial year i.e. October to March in succeeding May in every Financial Year.

5.2.8 Risk Rating of customer

Bank shall ensure to classify Customers as Low Risk, Medium Risk and High Risk depending on background, nature and location of activity, country of origin, sources of funds and customer profile etc.

A. An illustrative list of Low / Medium / High Risk Customers, Products, Services, Geographies, etc., based on recommendations of IBA Working Group on Risk Based Transactions Monitoring (detailed in Annexure III of this policy).

B. Risk rating based on the Deposits/account balance:

Account Types	**High**	**Medium**	**Low**
All deposit accounts (SB+ CA+ TD)	Rs. 100 lakh & above	Rs. 25 lakh & above but less than Rs. 100 lakh	Less than Rs. 25 lakh

Above categorization of the Customer shall be based on all accounts linked to Customer Information File (CIF) irrespective of constitution of account like Joint account, Partnership account etc. However, accounts linked to (CIF) where customers do not have any stake in Business / activity need not be clubbed for the above purpose.

C. Risk Categorization of the customers shall be done according to the risk perceived while taking into account the above aspects. For instance, a salaried class individual who is generally to be classified under low risk category may be classified otherwise based on following illustrative list of parameters considered as "High Risk" such as:

- Unusual transaction / behaviour.
- Submitted Suspicious Transaction Reports (STR) for Customer.
- Submitted Cash Transaction Report (CTR).
- Frequent Cheque returns.
- Minor

D. Risk categorization of customers shall be based on combination of above parameters, i.e., mentioned under A, B & C above. Among the chosen parameters, highest risk grade will be assigned as overall Risk for the customer.

Example: a Travel Agent (Medium risk) with Proprietorship account (Medium risk) and having Savings account with average balance of Rs. 1,50,000/- (Medium risk) and Term Deposit of Rs. 4,00,000/- (Low risk), shall be assigned with overall rating of "Medium Risk", provided all other conditions mentioned under C above does not necessitate for assigning "High Risk".

5.2.9 Customer Due Diligence (CDD) for Virtual Currencies (VCs)

Branches need to remain vigilant and ensure enhanced due diligence are in place while dealing with such entities and their customers. Full Compliance of PML Act/Rules and the Master Direction on KYC should be ensured for any such relationship.

Banks to ensure following while transactions with entities dealing with VCs entities.

I. All Customers dealing in VCs should be categorized as High Risk
II. Ensuring highest degree of vigilance while undertaking such transactions
III. Ensuring enhanced due diligence while dealing with entities /customers engaged in VCs
IV. Identification of Beneficial Owner (BOs) where ever applicable.

5.2.10 Risk categorisation of customers undertaken by the bank

Based on the policy / guidance / notifications of RBI / IBA and also the methodology of Customer Risk Categorization (as detailed under points A, B & C above), risk rating has been assigned taking into account the following parameters available in CBS system:

i. Customer type
ii. Customer constitution.
iii. Type of business.
iv. Product code.
v. Account status
vi. Account vintage
vii. Average balance in deposits in SB / Current / Term Deposit accounts.

All customer profiles / accounts of NRIs, HNIs, PEPs, NGOs, Trusts, Co-operative Societies, HUF, Exporters, Importers and Accounts having Beneficial Owners shall be invariably categorized as High Risk, irrespective of the lower risk category (low / medium) allotted under other parameters in the Matrix like customer profession, type of business, product code, account status, account vintage and balance in the account.

As per RBI directions, the parameters used for categorizing the risk profile of customers should include those named in complaints (from legal enforcement authorities) / frauds. As the system will not identify the customers / accounts named in complaints (from legal enforcement authorities) / frauds, this parameter has not been included in the Risk

Categorization Matrix: Branches are advised to categories such customers / accounts under “High Risk” category as and when complaints (from legal enforcement authorities) are received or fraud is reported against the customer / account holder.

Blocked Accounts and Unclaimed deposits shall be categorized as High Risk. As per RBI directions, Blocked account status should be part of the initial categorization of an account at the branch level rather than being part of the review of risk categorization at the central level. Hence, branches are advised to categories such accounts as High Risk at the time of blocking the account.

Accounts of dealers in Jewellery, Gold / Silver / Bullions, Diamonds and other precious metals / Stones shall be categorized under “High Risk”.

Under vintage parameter, newly opened CASA accounts which have not completed 6 months shall be categorized as High Risk, except accounts pertaining to staff, ex-staff, pensioners, small accounts, Financial Inclusion and Basic Savings Bank Accounts. However, if the accounts under the above categories are rated as High / Medium risk under any of the other 6 parameters under the risk categorization matrix, such accounts are to be categorized basing on the highest risk category allotted under those parameters.

Once new account completes six months then the account should be categorized as medium subject to complying with other parameters. Account thereafter should go to low risk after twelve months subject to complying with other parameters.

5.2.11 Money Laundering and Terrorist Financing Risk Assessment by Bank:

(a) IRM Department HO shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.
The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, IRM Department, HO 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 shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Bank. Further, the periodicity of risk assessment exercise shall be determined by the Board, 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 Risk Management Committee of the Board, 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 identified risk and should have Board approved policies, controls and procedures in this regard. Further, Bank shall monitor the implementation of the controls and enhance them if necessary. IRM Department HO shall issue separate guidelines & SOP in this regard.

5.2.12 Roles & Responsibilities (Compliance of the Policy)

i. Designated Director

Bank has nominated the Executive Director as a Designated Director of the Bank, as required, to ensure overall compliance with the obligations under the Act and Rules. The Designated Director shall oversee the compliance position of AML norms in the Bank.

The name, designation and address of the Designated Director shall be communicated to the FIU-IND as well as RBI.

ii. Principal Officer

Bank has appointed General Manager, Inspection and Audit, Head Office as Principal Officer. The Principal Officer shall be independent and report directly to the senior management or to the Board of Directors.

Principal Officer is responsible for monitoring AML compliance at operational units, escalation of suspicious transactions reported by branches through STRs and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

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

The Principal Officer is responsible for timely submission of STR, CTR, CBWTR and reporting of counterfeit notes (CCR) and all transactions involving receipts by Non-Profit Organizations (NTR) of value more than Rupees Ten lakh or its equivalent in foreign currency to FIU-IND.

The Principal Officer and other appropriate staff shall have timely access to customer identification data and other CDD information, transaction records and other relevant information.

The Principal Officer shall be the competent authority for fixing the thresholds for generation of AML alerts and the periodicity of reviewing the alerts shall be once in a year or as and when required.

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

iii. Chief Operating Officer

a. Chief Operating Officer shall be head of Operation department and shall be responsible for monitoring KYC/ CKYC / R-KYC / V-KYC compliance at operational units, The role and responsibilities of the Chief Operating Officer include overseeing and ensuring overall compliance with regulatory guidelines on KYC/ CKYC / R-KYC / V-KYC issued from time to time and, rules and regulations made there under, as amended from time to time
b. Operation Department shall identify the parameters available in the system for risk categorization through the system as per the model suggested in the policy.
c. Operation Department shall review fixing of parameters available through the system half yearly from PMO Department.
d. Operation Department will review on risk categorization of all CIFs and accordingly generate the alerts through CBS for periodic updation of KYC (Re-KYC) to eligible customers and monitoring of the same in liaison with IT Department.
e. Operation department shall submit quarterly report to the Board/ ACB.

f. Operation department shall ensure the compliance of directions given by the Audit Committee of the Board.
g. Bank shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.
h. Operation Department shall follow up with the Zones & branches for identification & updation of Beneficial Owner (BO) in all eligible Legal Entity accounts.

iv. Planning Department:

Issuance of guidelines pertaining to KYC/AML/CFT for Domestic deposits for all deposit products through deposit policy and implementation / monitoring of the same in liaison with IT Department.

v. Operations Department:

Issuance of guidelines pertaining to KYC/ CKYC / R-KYC / V-KYC and implementation thereon for all existing and new accounts and monitoring of the same in liaison with IT Department.

Operations Department shall review and provide necessary recommendations / directions to strengthen adherence of KYC/AML guidelines

vi. TIBD:

Issuance of guidelines pertaining to KYC/AML/CFT for Overseas deposits and implementation / monitoring of the same in liaison with IT Department.

vii. PMO, IT Department, H.O

a. IT Department shall identify the parameters available in the system for risk categorization through the system as per the model suggested in the policy in liaison with Operation Department
b. PMO Shall review fixing of parameters available through the system half yearly.
c. PMO Shall conduct risk categorizations of all CIFs in our CBS for the first half of the financial year i.e. April to September shall be undertaken in succeeding November and for second half of the financial year i.e. October to March in succeeding May in every Financial Year in liaison with Operation Department.
d. IT may also apply additional alert indicators to address specific risks faced and informed by AML Cell.
e. Add Update the UAPA List SDN List as and when provided by the AML list and real time screening with list before and applying stop, override in all matching cases.

viii. AML cell, Inspection & Audit Department H.O.

Verification of implementation of AML/CFT guidelines including liaison with RBI/IBA/FIU/other agencies, reporting to regulatory authorities and RBI apart from attending to STR, CTR, NTR and CCR alerts.

The AML cell take steps to identify and assess the Money Laundering / Terrorism Financing risk for customers, as also for products / services / transactions / delivery channels. Bank shall have controls and procedures in place to effectively manage and mitigate the risk adopting a risk-based approach. As a corollary, AML cell adopt enhanced measures for products, services and customers with a medium or high-risk rating.

a. Shall assess periodical AML/CFT and reporting to Top-Management / Board.

b. HO AML cell is responsible for scrutiny / closure of STR alerts and submission of CTR / NTR / CBWTR / CCR / STR to FIU-IND. Post-Closure scrutiny of closed alerts @5 % shall be undertaken by officials in cadre SMG-IV or above,

c. AML cell is also responsible for attending queries raised by FIU-IND, Enforcement Directorate, and other Law Enforcement Agencies, and reporting to Top-Management / Board,

d. AML Cell shall attend correspondent banking questionnaires in liaison with TIBD after duly vetted by Chief Compliance Officer of the Bank.

ix. Roles and responsibilities of Inspection & Audit Department, HO

a. Shall specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard.

b. 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. At the end of every calendar quarter, implementation and compliance of concurrent audit reports on adherence to KYC-AML guidelines at branches would be reviewed for apprising Audit Committee of Board.

x. Roles and responsibilities of Zonal Offices

a. Shall monitor / follow-up process of review / classification / re-classification of Customer Risk Categorization.

b. Zonal Manager shall be responsible for monitoring KYC / AML / CFT/ CKYC / Re-KYC compliance at operational units, including overseeing and ensuring overall compliance with regulatory guidelines on KYC / AML / CFT / CKYC / Re-KYC in the Zone , abiding by the policy guidelines and govt rules and regulations , as amended from time to time .

c. Shall ensure implementation of KYC-AML guidelines by branches in letter and spirit, has to be ensured by Zonal Managers / Deputy Zonal Managers and the same is to be checked during their visit to branches.

d. Shall attend / follow-up audit observations/remarks.

e. Shall follow up with the branches and ensure compliance for identification of Beneficial Owner in Legal Entity Accounts & Updation in CBS system.

xi. Roles and responsibilities of Branches

a. Wherever there is suspicion at branch level that customer is above low risk, branches should carry out customer due diligence (CDD).

b. Functionality for raising suspicious transactions at branch level has been provided in ULC dropdown under the name of AML Offline Scenarios, where branches can raise suspicion on selection of relevant RFIs (Red Flag Indicators) and uploading KYC documents & AOF.
c. Suspicious transactions based on adverse media reports & Law Enforcement Agency enquires, public complaints, behavioural scenarios, attempted transactions etc. Shall be escalated to Centralized AML Cell through AML offline Scenarios Module /email.
d. While monitoring of transactions, branches shall arrive at a conclusion whether the transaction is suspicious or not, based on objective parameters for enhanced due diligence. Some of the objective parameters for enhanced due diligence should be:
   - Customer locations
   - Financial status
   - Nature of business
   - Purpose of transaction.
e. Branches are responsible for ensuring compliances of KYC/AML/CFT guidelines in letter and spirit.
f. Branch shall ensure to identify beneficial owner in Legal Entity Accounts & update the same in CBS System for all new as well as existing legal entity accounts.
g. Branch Manager shall be responsible for monitoring KYC / AML / CFT/ CKYC / Re-KYC compliance at operational units, including overseeing and ensuring overall compliance with regulatory guidelines on KYC / AML / CFT / CKYC / R-KYC in the Branch , abiding by the policy guidelines and govt rules and regulations , as amended from time to time .
h. Branch shall ensure to complete CKYC and Re-KYC in all eligible accounts.

It shall be the duty of every bank branch, its Designated Director, officers and employees to observe the procedure and manner of furnishing and reporting information on transactions.

5.2.13 Monitoring / Review of Customer Risk Categorization (CRC)

Please refer **Annexure IV for Monitoring / Review of Customer Risk Categorization (CRC)** in detail.

5.3 Customer Identification Procedure (CIP)

Customer identification means undertaking CDD (Customer Due Diligence i.e. identifying and verifying the customer and the beneficial owner).

a. Bank shall obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of banking relationship. The Bank shall observe due diligence based on the risk profile of the customer in compliance with the extant guidelines in place. Besides risk perception, the nature of information / documents required would also depend on the type of customer (individual, corporate, etc.).
b. Bank shall clearly spells out the Customer Identification Procedure to be carried out at different stages, i.e.
   i. While establishing a banking relationship;

ii. While carrying out a financial transaction;

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

iv. When the Bank has a doubt about the authenticity or adequacy of the customer identification data it has obtained;

v. When bank sells third party products as agent;

vi. While selling Bank's own products, payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product for more than Rs. 50,000/-.

vii. When carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount is equal to or exceeds Rs. 50,000/- whether conducted as a single transaction or several transactions that appear to be connected;

viii. When the Bank has reason to believe that a customer (account based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000/-.

ix. Bank shall ensure that introduction is not to be sought while opening accounts.

'Mandatory' information required for KYC purpose which the customer is obliged to give while opening an account should be obtained at the time of opening the account / during periodic updation.

Customer Due Diligence requirements (CDD) while opening accounts

CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR) : Branches shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individual and Legal Entities' as the case may be. Government of India has authorized the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification dated November 26, 2015.

While establishing an account based relationship with individual customer, the branch official to ascertain as to whether the customer is already having a Customer ID with the Bank. In case the customer has an existing Customer ID, fresh Customer ID shall not be created and the new account shall be opened with the existing Customer ID. The name, father's name, date of birth and address of the customer be filled in the same manner and style as it appears in the KYC document provided by the customer. Branch official will ensure that all the mandatory fields in Account Opening Form / Customer Master Form (marked as *) such as Name, Father's name, date of birth, address , Identity Proof , address proof, Identification number (Identity proof document number) , Profession / activity (Nature of Business -specific) , total annual income , total annual turnover (in case of business) etc. are completely and correctly filled in by the customer and are also correctly captured in customer's database in CBS. The respective division/ offices of the Bank shall ensure that branches are capturing correct data in CBS system, particularly in respect of Constitution Code, Profession/ Activity, Occupation, Income/ Turnover etc. as risk category of the customer is assigned on the basis of these parameters.

5.3.1 e-KYC services of UIDAI

In order to reduce the risk of identity fraud, document forgery and to have paperless KYC verification, UIDAI has launched its e-KYC service. The Reserve Bank of India has directed the banks to accept e-KYC service as a valid process for KYC verification under Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

Further, the information containing demographic details and photographs made available from UIDAI as a result of e-KYC process (which is in an electronic form and accessible so as to be usable for a subsequent reference) shall be treated as an Officially Valid Document under PML Rules.

i. Branches can continue to seek e-KYC based authentication of those beneficiaries who are availing subsidies / benefits / services owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, bank shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD or the equivalent e- document thereof from the customer.
ii. CDD done in this manner shall invariably be carried out by an official of the bank branch and such exception handling shall also be a part of the concurrent audit.
Bank 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 authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit / inspection by the bank and shall be available for supervisory review.
iii. e-KYC authentication facility can also be continued to be permitted for those customers who give a declaration that s/he is desirous of receiving her/his entitled benefits or subsidies of welfare schemes such as scholarship, mid-day meals, LPG subsidies, free education.
iv. For other customers, Branches can use physical copy of the Aadhaar card as well as eAadhaar, masked Aadhaar and offline electronic Aadhaar xml provided by UIDAI, which are various forms of Aadhaar, as Officially Valid Documents (OVD) for the KYC purpose.

(As per UIDAI circular dated 23-10-2018 based on the opinion received from the Ld. Attorney General for India after the Aadhaar Judgment of the Hon. Supreme Court of India, delivered on 26-09-20 18).

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

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

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

5.3.1.A Manner of voluntary use of aadhaar number

a) An Aadhaar number holder may voluntarily use the Aadhaar number in physical form, including Aadhaar letter (or copy thereof) or printed e-Aadhaar or Aadhaar PVC Card for a lawful purpose for establishing his identity by way of offline verification and the branch shall verify the printed details on Aadhaar letter or printed e-Aadhaar or Aadhaar PVC card with digitally signed Aadhaar Secure QR code12.

b) An Aadhar number holder may voluntarily use the Aadhaar number in electronic form, including e-Aadhaar or Aadhaar Paperless Offline e-KYC (XML) or m-Aadhaar for a lawful purpose for establishing his identity by way of offline verification and the branch shall verify the digital signature.

c) An Aadhaar number holder may voluntarily use the Aadhaar number in electronic form by way of authentication for a lawful purpose for establishing his identity by way of Yes/No or eKYC authentication facility through an authorized requesting entity.

5.3.1.B Conditions for accepting an Aadhaar number as proof of identity

a) branches shall not accept Aadhaar number, in physical or electronic form (without authentication), as a proof of identity for a lawful purpose, without first verifying the digital signature of the Authority as provided in the Aadhaar secure QR Code on Aadhaar Letter or e-Aadhaar or m-Aadhaar or Aadhaar Paperless Offline e-KYC (XML), as the case may be.

b) No branch shall accept Aadhaar number as a proof of identity of the Aadhaar number holder, in electronic form by way of authentication, unless it is for a lawful purpose which is in conformity with the relevant provisions of the Act and only with the informed consent of the Aadhaar number holder and in a manner as provided in the Aadhaar (Authentication and Offline Verification) Regulations, 2021."

5.3.2 Introduction of accounts

Since introduction from an existing customer is not necessary for opening accounts under PML Act and Rules or the RBI's extant instructions, branches shall not insist on introduction for opening of bank accounts. After passing of PML Act and introduction of document based verification of identity / address of the proposed account holders, the accounts opened with proper documents are considered as acting in good faith and without negligence by the banks.

5.3.3 Accounts of individuals

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

A. The Aadhaar number where,
   i. the customer is desirous of receiving any benefit or subsidy, benefit or service for which the expenditure is incurred from, under any scheme notified by Central Government or State Government; or

ii. The customer decides to submit his Aadhaar number voluntarily to a bank without consultation with the Unique Identification Authority of India; or

a. The proof of possession of Aadhaar number where offline verification can be carried out; or

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

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

C. Such other documents in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the bank.

i. Aadhaar number under clause (A) above, branch shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India.

Further, in such case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the bank.

ii. Proof of possession of Aadhaar under clause (a) above where offline verification can be carried out, the bank shall carry out offline verification.

iii. An equivalent e-document of any OVD, the bank shall verify the digital signature and take a live photo as specified under **Annexure I**.

iv. Any OVD or proof of possession of Aadhaar number under clause (b) above where offline verification cannot be carried out, the bank shall carry out verification through digital KYC as specified under **Annexure I**.

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

5.3.4 Accounts of married woman

As per the amendment to the Rules, 2005 (Gazette notification dated 22.09.2015), a document shall be deemed to 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.

Accordingly, Branches shall accept a copy of marriage certificate issued by the State Government or Gazette notification indicating change in name, together with a certified copy of the 'Officially Valid Document' in the existing name of the person while establishing an account based relationship or while undergoing periodic updation exercise.

5.3.5 Small Accounts

It has been observed that a large number of persons, especially, those belonging to low income group both in urban and rural areas are not able to produce Officially Valid Documents (OVDs) to

satisfy the Bank about their identity and address. This would lead to their inability to access the banking services and result in their financial exclusion. In such cases, if a person who wants to open an account and is not able to produce any of the OVDs or the documents applicable in respect of simplified procedure, bank shall open a small account. The small accounts can be opened under "Maha Bank Lok Bachat Yojana".

The small account can be opened by production of a Self-attested photograph and affixation of signature or thumb impression, as the case may be, on the Account Opening form. The designated branch official, while opening the small account, should certify under his signature that the person opening the account has affixed his signature or thumb impression as the case may be, in his presence.

The features of the above account and limitations stipulated by RBI / Govt. of India are as follows:

i. accounts where aggregate of all credits in a financial year does not exceed Rs. 1.00 Lakh;

ii. The aggregate of all withdrawals and transfers in a month does not exceed Rs. 10,000/- and

iii. Where the balance at any point of time does not exceed Rs. 50,000/-.

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

Bank shall ensure that the stipulated monthly and annual limits on aggregate of transaction and balance requirements in such accounts are not breached, before a transaction is allow to take place.

Any violation of the stipulations mentioned above will result in restraining the operations in the account after giving due notice to the account holder.

The 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 before the Bank 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.

Notwithstanding, the small account small remain operational between April 1, 2020 and June 30, 2020 and such other periods as may be notified by the Central Government.

The small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of customer shall be established through the production of certified Officially Valid Documents.

Foreign remittances shall not be allowed to be credited into a small account unless the identity of the customer is fully established through the production of officially valid documents.

5.3.6 Accounts of Prisoner in a Jail

In respect of the individual who 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.

a. Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account.
b. Such accounts shall be opened in small accounts product only and all the limitations stipulated by RBI / Govt. of India shall be applied.

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

5.3.7 Basic Savings Bank Deposit Accounts

As per RBI guidelines, the Basic Savings Bank Deposit Account shall be considered a normal banking service available to all.

The Basic Savings Bank Deposit Account would be subject to RBI instructions on Know Your Customer (KYC) /Anti-Money laundering (AML) for opening of bank accounts issued from time to time.

5.3.8 Customer Due Diligence requirement (CDD) by Third Party

For the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship, the branch may rely on a third party; subject to the condition that :

a) Records of the information of the customer due diligence carried out by the third party is obtained within two days from the third party of from the Central KYC Records Registry.
b) The 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 third party is not a based in a country or jurisdiction assessed as high risk; and
d) The branch is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

5.3.9 Accounts opened using OTP based e-KYC, in non-face-to-face mode

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

i. There must be a specific consent from the customer for authentication through OTP.
ii. As a risk-mitigating measure for such accounts, bank shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar. Bank has approved policy delineating a robust process of due diligence for dealing with requests for change of mobile number in such accounts. Request for change in mobile number shall only be accepted where mobile number has been updated in aadhaar number. It must be noted that mobile number linked with aadhaar number and for transactions alerts should be the same.

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

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

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

vi. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which identification is to be carried out, **as per para 5.3.1.**

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

viii. A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non- face-to-face mode with any other bank. Further, while uploading KYC information to CKYCR, the bank shall clearly indicate that such accounts are opened using OTP based e-KYC and 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.

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

5.3.10 Video based Customer Identification Process (V-CIP)

Accounts, both deposit and borrower, opened using OTP based e-KYC shall not be allowed for more than one year unless identification as per Section 16 or as per Section 18 (V-CIP) is carried out, If Aadhaar details are used under Section 18, the process shall be followed in its entirety including fresh Aadhaar OTP authentication

Bank may undertake V-CIP to carry out:

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

Provided that in case of CDD of a proprietorship firm, REs shall also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in Section 28 and Section 29, apart from undertaking CDD of the proprietor.

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

Iii) Updation/Periodic updation of KYC for eligible customers

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

(a) V-CIP Infrastructure

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

2. The Bank shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer consent should be recorded in an auditable and alteration proof manner.
3. The V-CIP infrastructure / application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.
4. 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.
5. The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Bank. Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust
6. 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-security event under extant regulatory guidelines.
7. 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 empanelled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.
8. The V-CIP application software and relevant APIs / web services shall also undergo appropriate testing of functional, performance, and maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines

b) V-CIP Procedure

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

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

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

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

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

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

a) OTP based Aadhaar e-KYC authentication
b) Offline Verification of Aadhaar for identification
c) KYC records downloaded from CKYCR, in accordance with Section 57, using the KYC identifier provided by the customer
d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker

Bank shall ensure to redact or blackout the Aadhaar number in terms of Section 16 where the authentication of Aadhaar number is not required.

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

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

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

VIII) The authorised official of the Bank performing V-CIP shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digilocker.

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

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

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

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

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

c) **V-CIP Records and Data Management.**

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

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

5.3.11 Accounts of Proprietary Concerns

For Proprietary concerns, Customer Due Diligence of the Individual (Proprietor) is to be carried out and any two of the following documents or the equivalent e- documents there of as a proof of business / activity in the name of the proprietary firm should be obtained:

a. Registration Certificate, including Udyam Registration Certificate (URC) issued by the Government.
b. Certificate / license issued by the Municipal authorities under Shop & Establishment Act.
c. Sales and income tax returns.

d. CST / VAT / GST certificate.
e. Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities.
f. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
g. Complete Income Tax return (not just the acknowledgement) in the name of the sole Proprietor where the firm's income is reflected, duly authenticated / acknowledged by the Income Tax Authorities.
h. Utility bills such as electricity, water and landline telephone bills of firm.

Though the default rule is that any two documents mentioned above should be provided as activity proof by a Proprietary concern, in cases where the branches are satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the branches, however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern. Photograph should be obtained in case of NRI accounts also.

5.3.12 Accounts of Legal Entities (Other than Individuals)

Bank need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. Bank shall examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

A. Accounts of Companies

Where the customer is a company, certified copies of all the following documents or the equivalent e-documents shall be obtained:

i. Certificate of incorporation
ii. Memorandum and Articles of Association
iii. Permanent Account Number of the Company
iv. A resolution from the Board of Directors and Power of Attorney granted to its managers, officers or employees to transact on its behalf.
v. **One copy of an officially Valid Document (OVD) containing details of identity and address, one recent photograph and Permanent Account Numbers or Form 60 of related beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf. Complete Due Diligence of all such individuals has to be undertaken.**
vi. The names of the relevant persons holding senior management position; and
Vii.The registered office and the principal place of its business, if it is different.

B. Accounts of Partnership firms

Where the customer is a partnership firm, certified copies of all the following documents or the equivalent e-documents shall be obtained:

i. Registration Certificate

ii. Partnership Deed
iii. Permanent Account Number of the Partnership Firm
iv. One copy of an officially Valid Document (OVD) containing details of identity and address, one recent photograph and Permeant Account Numbers or Form 60 of related beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the it's behalf;
v. The names of all the partners and address of the registered office, and the principal place of its business, if it is different.

C. Accounts of Trusts

Where the customer is a Trust, certified copies of all the following documents or the equivalent e-documents thereof shall be obtained:

i. Registration Certificate
ii. Trust Deed
iii. Permanent Account Number or Form 60 of the Trust
iv. One copy of an officially Valid Document (OVD) containing details of identity and address, one recent photograph and Permanent Account Numbers or Form 60 of related beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.
vi. The names of beneficiaries, trustees, settlor and authors of the trust and the address of the registered office of the trust: and
Vii.List of trustees and documents as are required for individuals under sub-rule (4) for those discharging role as trustee and authorized to transact on behalf of the trust.

D. Accounts of Unincorporated association or a body of individuals

Where the customer is an unincorporated association or a body of individuals, certified copies of all the following documents or the equivalent e- documents thereof shall be obtained:

i. Resolution of the managing body of such association or body of individuals

ii. Permanent Account Number or Form 60 of the Unincorporated association or a body of individuals

iii. Power of Attorney granted to the person who will transact on its behalf.

iv. One copy of an officially Valid Document (OVD) containing details of identity and address, one recent photograph and Permanent Account Numbers or Form 60 of related beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf and

v. Such information as may be required by the branch to collectively establish the legal existence of such an association or body of individuals.

Note:

a. Unregistered trusts / partnership firms shall be included under the term **'unincorporated association'.**
b. Term 'body of individuals' includes societies.

E. For opening accounts of Governments or its Departments, Societies, Universities and Local Bodies like Village Panchayats (Juridical persons)

The certified copies of all the following documents or the equivalent e- documents shall be obtained:

i. Document showing name of the person authorized to act on behalf of the entity;

ii. Any Officially Valid Document (OVD) which contains proof of identity and address in respect of person holding an attorney to transact on the company's behalf and

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

H. Opening of Current Account.

For opening of current account refer RBI guidelines vide letter No.-RBI letter no.-DOR.CRE.REC.63/21.04.048/2021-22 October 29 (Opening of Current Accounts by Banks - Need for Discipline**. Bank has also issued circular No.-AX1/CrMon/CA/19/2021-22 dated 30.10.2021 and SOP in this regard.**

I. Accounts of Non Profit Organizations

A 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 At, 1961 (43 of 1961), that is registered as a Trust or a Society under the Societies Registration Act, 1860 (21 of 1860) or any similar State Legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).

All transactions involving receipts by these NPOs of value more than Rs. 10 Lakh or its equivalent in foreign currency is to be reported to FIU-IND centrally from Head Office. However, if the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 10 lakh, the Bank shall consider filing a Suspicious Transaction Report to FIU-IND.

Registration of NPO (Non-profit Organization) on the DARPAN Portal of NITI Aayog

Bank shall register the details of non-profit organisation on the DARPAN Portal of NITI Aayog, and shall maintain such registration records for a period of five years after the business relationship has ended or the account has been closed, whichever is later. Operation Department shall issue separate guidelines and SOP in this regard.

J. Accounts operated by Power of Attorney Holders / Letter of Authority Holders

In case of accounts operated by Power of Attorney (POA) Holders / Letter of Authority (LOA) Holders, KYC documents shall be obtained from such POA holders/ LOA holders and records shall be maintained/ updated in the system.

Where the accounts are operated by letters of authority, photographs of the authority holders should be obtained, duly attested by the depositors.

5.3.13- Identification of Beneficial Owner (BO) in Legal Entity Accounts:

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) Bank is required to identify BO (Beneficial ownership) in accounts of Company, Partnership firm, unincorporated associations and Body of Individual and update in CBS System, separate guidelines/SOP/FAQs in this regard is already issued by the Bank.

(b) Where the customer or the owner of the controlling interest is a company listed on a stock exchange, or it is an entity resident in jurisdictions notified by the Central government and listed on stock exchanges in such jurisdictions, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

(c) 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.

5.3.14 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 60/61 shall be obtained from persons who do not have PAN or equivalent e-document thereof.

5.3.15 Need for photographs and address confirmation

Passport size / stamp size photograph of the depositors shall be obtained in case of all Current Accounts, SB accounts and Term Deposits.

In case of joint accounts, partnership accounts, accounts of societies, clubs, associations, public / private limited companies, HUF, trusts, Limited Liability Partnerships etc., and those of minors, photographs of the authorized signatories should be obtained. Photographs of the student account holders should be attested by the school authorities on the reverse. In case of change in the authorized signatories, photographs of the new signatories are to be obtained duly countersigned by the competent authorities of the concerned institutions/ organizations.

5.3.16 Introduction of New Technologies - Credit cards / debit cards / smart cards / gift cards etc.

Bank shall pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favor anonymity, and take measures, if needed, to prevent the same being used for money laundering/terrorist financing purposes. The Electronic Cards (debit card, credit card, etc.) issued by the Bank to the customers may be used by them for buying goods and services, drawing cash from ATMs and electronic transfer of funds.

Branch shall ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. Branch shall ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Further, where marketing of these cards is done through the services of agent, the agents will also to be subjected to due diligence and KYC measures.

Further, Bank shall ensure

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

5.3.17 Periodic Updation of KYC

Bank shall adopt a risk-based approach for periodic updation of KYC. However, periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers from the date of opening of the account / last KYC Updation.

A. CDD (Customer Due Diligence) requirements for periodic updation:

i. 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 Bank), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc. Further, Branch shall obtain a copy of OVD or the equivalent e-documents thereof, as defined in Section 4.9 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 may be used for periodic updation. To clarify, conditions stipulated in Section 17 are not applicable in case of *updation* / *periodic updation of KYC* through Aadhaar OTP based e-KYC in non-face to face mode.

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

ii. Customers other than individuals:

a) No change in KYC information: In case of no change in the KYC information of the LE (Legal Entity) 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 LE customer.

iii. 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 Branch 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, Branch 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) Fresh KYC process can be done by visiting a bank branch, or remotely through a Video based Customer Identification Process (V-CIP)

d) 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 the CBS System and an intimation through emails/messages, mentioning the date of updation of KYC details, is provided to the customer.

d) **In cases where individual customers express difficulty in approaching the home branch due to age related and other issues, such customers may approach the Branch Head of non-home Branch, who shall obtained the necessary KYC documents along with the details as per bank format from the customer, attest the same and immediately send to home branch for updation in CBS.**
In case of Legal Entity / Corporate customers, collection of KYC details for Re-KYC and updation of the same in CBS is to be done at Home-Branch only

Bank shall ensure to provide acknowledgement with the date of having performed KYC updation.
e) Bank shall advise the customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship

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

B. CDD Procedures and sharing KYC information with Centralize KYC Records Registry (CKYCR)

Government of India has authorized the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI) to act as and to perform the functions of the CKYCR vide Gazette Notification dated November 26, 2015.

Bank shall capture the KYC information for sharing the CKYCR 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.

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

Once identifier is generated by CKYCR, bank shall ensure that the same is communicated to the individual / Legal Entity as the case may be.

Where a customer, for purposes of establishing an account based relationships, submits a KYC identifier to a bank, with an explicit consent to download records from CKYCR, then such bank shall re-retrieve the KYC records online form CKYCR using KYC identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless

a. There is change in the information of the customer as existing in the records of CKYCR;
b. The current address of the customer is required to be verified;
c. In order to verify the identity and address of the customer, or to perform enhanced due diligence or to build an appropriate risk of the client.

Branches shall ensure that during periodic updation, the customer are migrated to the current CDD standard.

In order to ensure that all KYC records are incrementally uploaded on to CKYCR, branches shall upload / update the KYC data pertaining to accounts of individual customers and Legal Entities opened prior to January 2017 at the time of periodic updation or earlier when the updated KYC information is obtained / received from the customer.

Branches shall upload KYC records pertaining to accounts of Legal Entities opened on or after April 1, 2021, on to CKYCR in terms of the provisions of Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

C. Temporary ceasing of operations

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

Before temporarily ceasing operations for an account, the bank shall give the customer an accessible notice and a reasonable opportunity to be heard. Further, appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or 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.

If a customer having an existing account-based relationship with bank and gives in writing to the bank that he does not want to submit his Permanent Account Number or Form No. 60, bank shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

"Temporary ceasing of operations" in relation an account shall mean the temporary suspension of all transactions or activities in relation to that account by the bank till such time the customer complies. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

D. Freezing and Closure of accounts

It would always be open to the Bank to close the account of KYC non-compliant customers after issuing due notice to the customer explaining the reasons for taking such a decision.

Such decisions need to be taken by the Branch Manager.

While it is absolutely necessary for banks as well as customers to comply with the measures prescribed for KYC/AML purposes, drastic measures like closing of accounts may be taken only after sending out sufficient discernible warning signals to the customers, basing on the level of customer education and public awareness on the subject. In all such cases where the account holders are either not responding over a period of time/not found at the given address, Bank may take such action as deemed necessary to comply with KYC/AML guidelines without denying basic banking facilities.

Before taking the extreme step of closing an account on account of non-compliance with the KYC/AML requirements, as an initial measure, branches are advised to place such accounts under close watch, depriving the non-compliant customers certain additional facilities, till the customer complies with such requirements.

This exercise, however, should not extend beyond a period of three months. If the customer despite such measures, shows unwillingness to comply with KYC/AML/CFT requirements, branches would be free to proceed further and close the accounts after giving due notice to him/her. It is reiterated that basic banking transactions already in force should not be disturbed for meeting KYC review requirements.

In case of non-compliance of KYC requirements by the customers despite repeated reminders by branches, branches should impose "partial freezing" on such KYC non-compliant accounts in a phased manner. Meanwhile, the account holders can revive accounts by submitting the KYC documents as per instructions in force. While imposing "partial freezing", branches are advised to

ensure that the option of "partial freezing" is exercised after giving due notice of three months initially to the customers to comply with KYC requirements and followed by a reminder for further period of three months. Thereafter, branches to impose "partial freezing" by allowing all credits and disallowing all debits, with the freedom to close the accounts.

If the accounts are still KYC non-compliant after six months of imposing initial "partial freezing", branches should disallow all debits and credits from/to the accounts, rendering them inoperative. Further, it would always be open to the branches to close the account of such customers after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions, however, need to be taken by the Branch Manager. In the Circumstances when the Bank believes that it would no longer be satisfied about the true identity of the account holder, the Bank shall file a Suspicious Transaction Report (STR) with Financial Intelligence Unit India (FIU-IND) under the Department of Revenue, Ministry of Finance, and Government of India.

Enhanced and Simplified Due Diligence Procedure

A- Enhanced Due Diligence

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

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

Non-face-to-face onboarding facilitates the banks to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section includes use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. Following EDD measures shall be undertaken by bank for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 5.3.9)

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

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

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

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

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

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

5.3.19 Accounts of Politically Exposed Persons (PEPs) :

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

Bank shall gather sufficient information on any person / customer of this category intending to establish a relationship and check all the information available on such person in the public domain. Bank shall verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. Bank shall also subject such accounts to enhanced monitoring on an ongoing basis. The above norms should also be applied to the accounts of the family members or close relatives of PEPs.

The decision to open an account of a PEP as well as the decision to continue the business relationship in the event of an existing customer or relatives of an existing customer subsequently becoming Politically Exposed Person (PEP), has to be taken at Zonal Office level by Zonal Manager or Deputy Zonal Manager.

In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the account shall be subjected to the Customer Due Diligence (CDD) measures as applicable to PEPs including enhanced monitoring on an ongoing basis. PEPs, customers who are close relatives of PEPs and accounts where a PEP is the ultimate beneficial owner shall be categorized as 'High Risk' so that appropriate transaction alerts are generated, and the accounts are subjected to enhanced CDD on an ongoing basis.

Bank shall have appropriate ongoing risk management systems for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner.

Zonal Offices shall closely monitor PEP accounts on ongoing basis for identifying and applying enhanced CDD to PEPs

<u>Separate occupation code 1008 is available in CBS for classifying customer as PEP</u>

5.3.20 Client accounts opened by professional intermediaries.

When the Bank has knowledge or reason to believe that the customer account opened by a professional intermediary is on behalf of a single client, that customer shall be identified.

Bank may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.

Branches shall not open accounts of such professional intermediaries who are bound by any customer confidentiality that prohibits disclosure of the customer details to the Bank. Where funds held by the intermediaries are not co-mingled at the Bank and there are 'subaccounts', each of them attributable to a beneficial owner, all the beneficial owners shall be identified. Where such funds are co-mingled at the Bank, the Bank shall still look into the beneficial owners.

Where the Bank rely on the 'Customer Due Diligence' (CDD) done by an intermediary, Bank shall satisfy itself that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers. The ultimate responsibility for knowing the customer lies with the Bank.

B-Simplified Due Diligence

5.3.21 Simplified norms for Self Help Groups (SHGs)

In order to address the difficulties faced by Self Help Groups (SHGs) in complying with KYC norms while opening Savings Bank accounts and credit linking of their accounts, following simplified norms shall be followed by branches:

i. KYC verification of all the members of SHGs need not be done while opening the Savings Bank account of the SHGs

ii. KYC verification of all the office bearers would suffice.

iii.KYC verification of all the members of SHG may be undertaken at the time of credit linking of SHGs.

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

5.3.22 Accounts of Foreign students studying in India

Considering that foreign students arriving in India are facing difficulties in complying with the Know Your Customer (KYC) norms while opening a bank account due to non-availability of any proof of local address, the following procedure shall be followed for opening accounts of foreign students who are not able to provide an immediate address proof while approaching the Bank for opening bank account:-

a. Branches may open a Non-Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.
b. Branches should obtain a declaration about the local address within a period of 30 days of opening the account and verify the said local address.
c. During the 30 days period, the account should be operated with a condition of allowing foreign remittances not exceeding USD 1000 or equivalent into the account and a cap of monthly withdrawal to Rs. 50,000/- and pending verification of address.

d. The account would be treated as a normal NRO account after verification of address and will be operated in terms of existing guidelines issued in the Manual of instructions on Non-Resident Deposits and Circulars issued from time to time.
e. Students with Pakistani nationality will need prior approval of the Reserve Bank of India for opening the account.

5.3.23 Simplified KYC norms for Foreign Portfolio Investors (FPIs) for Portfolio Investment Scheme (PIS)

Simplified norms have been prescribed for those FPIs who have been duly registered in accordance with SEBI guidelines and have undergone the required KYC due diligence / verification prescribed by SEBI through a Custodian / Intermediary regulated by SEBI. **Such eligible / registered FPIs may approach a bank for opening a bank account for the purpose of investment under Portfolio Investment Scheme (PIS) for which KYC documents prescribed by the Reserve Bank would be required subject to Income Tax (FATCA/CRS)**. Category-I FPIs are not required to submit the undertaking that upon demand by the Regulators/ Law Enforcement Agencies the relative document(s) would be submitted to the bank. **(Please refer Annex V)**

SEBI will advise Custodians/Intermediaries regulated by them to share the relevant KYC documents with the banks concerned based on written authorization from the FPIs. Accordingly, a set of hard copies of the relevant KYC documents furnished by the FPIs to the Custodians/Regulated Intermediaries may be transferred to the concerned bank through their authorized representative. While transferring such documents, the Custodian / Regulated Intermediary shall certify that the documents have been duly verified with the original or notarized documents have been obtained, wherever applicable. In this regard, proper records of transfer of documents have to be maintained, both at the level of the Custodian / Regulated Intermediary as well as at the bank, under signatures of the officials of the transferor and transferee entities.

While opening bank accounts for FPIs in terms of the above procedure, branches are ultimately responsible for the customer due diligence done by the third party (i.e. the Custodian/Regulated Intermediary) and need to take enhanced due diligence measures, as applicable, if required. Further, branches are required to obtain undertaking from FPIs or a Global Custodian acting on behalf of the FPI to the effect that as and when required, the exempted documents will be submitted.

In order to facilitate secondary market transactions, the branches may share the KYC documents received from the FPI or certified copies received from a Custodian / Regulated Intermediary with other banks/regulated market intermediaries based on written authorization from the FPI.

The above guidelines are applicable for both new and existing FPI clients. These guidelines are applicable only for Portfolio Investment Scheme (PIS) by FPIs. In case the FPIs intend to use the bank, account opened under the above procedure for any other approved activities (i.e. other than PIS), they would have to undergo full KYC exercise.

5.3.24 Miscellaneous

A. Period for presenting payment instruments

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

B. Collection of Account Payee Cheques

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

C. At par cheques facility availed by co-operative banks

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

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

(c) Cooperative Banks shall:

i. ensure that the 'at par' cheque facility is utilised only:
   a. for their own use,
   b. for their account-holders who are KYC complaint, provided that all transactions of rupees fifty thousand or more are strictly by debit to the customers' accounts,
   c. for walk-in customers against cash for less than rupees fifty thousand per individual.

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

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

D. Identification and Monitoring of Money Mule Accounts

Money Mules are individuals with bank accounts who are recruited by fraudsters to receive fund mostly through digital channels such as UPI, IMPS, Net Banking or wire transfer for the purpose of money laundering. "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." In order to prevent the misuse of the banking system by the fraudster and the money launderers through accounts of money mule, Branches should strictly adhere to the guidelines and apply appropriate CDD while opening of accounts and monitoring of transactions.

Any such account which has been flagged as suspected money mule accounts should immediately be subject to enhanced due diligence and enhanced monitoring without tip-off to the customer. Identified /suspected Money mule accounts should immediately be reported to Centralized AML Cell for onward reporting to FIU-IND.

E. Cybercrimes /frauds through investment / part time job /Ponzi scheme scams:

Incidence of a number of cybercrimes wherein the criminals and fraudsters are resorting to different kinds of modus operandi for perpetrating cybercrimes routed through banking channels and payment gateways are very high.

Some of the modus operandi followed by the fraudsters and criminals through investment / part time job / Ponzi schemes & preventive measures already issued by the bank vide circular no.-AX1/IRM/FMC/Cir.12/2022-23 **dated 18.10.2022.Bank has also shared certain specific location as shared by RBI where such frauds are more prevalent vide Circular No.-** AX1/IRMD/CISO/Cir. No.44/2021-22 dated 22/11/2021

Keeping in view the large number of cyber frauds and to prevent the misuse of the banking system by the fraudster and money launderers, branches are required to give special emphasis on strengthening the KYC / AML framework like adequate customer due diligence (including enhanced due diligence, wherever required) customer risk profiling and real time transaction monitoring. Make sure that accounts in the branches are not used as Money Mule Accounts for fund transfer

Continue to create awareness among customers for NOT sharing the OTP, login credentials and other banking security information and NOT to send money as initial deposit, commission or transfer fee to anyone claiming to provide huge usually unrealistic, return from known or unknown organizations/persons.

F. Walk-in Customers

In case of transactions carried out by a non-account based customer, i.e., a walk-in customer, where the amount of transaction is equal to or exceeds Rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address shall be verified.

If the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50000/-, the Bank shall verify identity and address of the customer and also consider filing a Suspicious Transaction Report to FIU-IND. The identity and address of the Walk-in customer shall be verified by obtaining KYC documents and records are to be maintained/ updated in the system. Bank shall also verify the identity of the customers for all international money transfer operations.

Types of transactions to be covered –

1. Cash deposit by third party in customer's accounts
2. Cash payment to walk-in customers
3. DD issued to walk-in customers
4. NEFT by walk –in customers

5. Sale of third party products viz.Insurance Policy, Mutual fund etc.

Bank has issued separate guidelines in this regard and entering the details of walk-in customers in CBS system vide circular no.- AX1/PLN/FI/KYC/Walk in Cust/79/2014-15 dated 30.09.2014.

G. Issue of Demand Drafts, etc., for more than Rs. 50,000/-

Any remittance of funds by way of Demand Draft, mail / telegraphic transfer / NEFT / IMPS or any other mode and issue of traveller's cheques for value of Rs. 50,000/- and above shall be effected by debit to the customer's account or against cheques and not against cash payment.

Bank shall not make payment of cheques / drafts / pay orders / banker's cheques if they are presented beyond the period of three months from the date of such instrument.

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 Bank with effect from September 15, 2018.

H. Sale of third-party products

When Bank sells third party products as an agent, the responsibility for ensuring compliance with KYC / AML / CFT regulations lies with the third party. However, to mitigate reputational risk to Bank and to enable a holistic view of a customer's transactions, branches are advised as follows:

i. While selling third party products as agents, branches should verify the identity and address of the walk-in customer.
ii. Branches should also maintain transaction details with regard to sale of third-party products and related records for a period and in the manner prescribed **in Point No. 8. (Maintenance of KYC documents and preservation period)**.
iii. Bank's AML software will capture, generate and analyse alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers.
iv. Sale of third-party products by branches as agents to customers, including walk-in customers, for Rs. 50,000/- and above must be

a. by debit to customer's account or against cheques and
b. Obtaining & verification of the PAN given by the account based as well as walk-in customers.

I. Issuance of Prepaid Payment Instruments (PPIs):

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

5.4 Monitoring of Transactions (On-going Due Diligence)

Ongoing monitoring is an essential element of effective KYC / AML procedures. Branches should exercise ongoing due diligence with respect to every customer and closely examine the transactions to ensure that they are consistent with the customer's profile and source of funds as per extant instructions. The ongoing due diligence may be based on the following principles:

a. The extent of monitoring will depend on the risk category of the account. High risk accounts have to be subjected to more intensify monitoring.
b. Branches should pay particular attention to the following types of transactions:
   i. Large and complex transactions, and those with unusual patterns, which have no apparent economic rationale or legitimate purpose.
   ii. Transactions which exceed the thresholds prescribed for specific categories of accounts.
   iii. Transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer.
   iv. High account turnover inconsistent with the size of the balance maintained.
   v. Deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts

   For ongoing due diligence, bank may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring
c. Bank put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorization of customers shall be carried out at a periodicity of not less than once in six months.
d. Branches closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies. Branches should analyze data in cases where a large number of cheque books are sought by the company, there are multiple small deposits (generally in cash) across the country in one bank account and where a large number of cheques are issued bearing similar amounts / dates. Where such features are noticed by the branches and in case they find such unusual operations in their accounts, the matter should be immediately reported to Reserve Bank and other appropriate authorities such as FIU-IND.
e. Supervisors should keep a vigil over the transactions involving huge amounts. Transactions should generally have a bearing with the occupation and /or line of business of the account holders. In case of any doubt, necessary enquiries should be made with the account holders.
f. While accepting the cheque for collection, it is to be ensured that the name mentioned in the challan and name of the beneficiary of the instrument are same.
g. Branches are advised to mandatorily obtain either PAN or Form 60/61 (if PAN is not available) for opening of accounts and also at the time of accepting cash receipt for Rs. 50,000/- and above. If the customer appears to be structuring the transactions into a serious of transactions below the threshold of Rs. 50,000/-, branches are required to obtain PAN or Form 60/61 (if PAN is not available) from the customer. Branches are advised to aggregate the split transactions across accounts of same customer to decide on the matter of obtention of PAN or Form 60/61, wherever the aggregate amount of transactions is Rs. 50,000/- and above.
h. All the staff members are instructed to maintain the standards of good conduct and behavior expected of them and not to involve in any activity that would bring disrepute to the institution and not to advise potential customers on the lines that would be an infringement of the legal

process/ could facilitate money laundering/ could defeat the KYC norms or the norms of due diligence prescribed by RBI from time to time.

6. Correspondent Banking and Shell Bank

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. Bank shall take the following precautions while entering into a correspondent banking relationship:

i. Bank shall gather sufficient information to fully understand the nature of the business of the bank including information on management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory / supervisory framework in the bank's home country, and publicly available information regarding the reputation of the institution and quality of supervision, including whether it has been subjected to ML/TF investigation or regulatory action, shall be gathered.
ii. Such relationships may be established only with the approval of the Board or by a committee headed by the MD & CEO with clearly laid down parameters for approving such relationships, as approved by the Board. Proposals approved by the Committee should be put up to the Board at its next meeting for post facto approval.
iii. The responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented.
iv. In the case of payable-through-accounts, Bank shall satisfy that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them.
v. Bank shall also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.
vi. Bank shall be cautious while continuing relationships with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of Financial Action Task Force (FATF) Recommendations.
vii. Bank shall ensure that its respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.
viii. Bank shall not enter into a correspondent relationship with a "shell bank" (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group).
ix. Bank shall not permit its accounts to be used by shell banks.

7. Wire Transfers

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

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

a. name of the originator;

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

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

d. name of the beneficiary; and

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 RE*, shall also be accompanied by originator and beneficiary information as indicated for cross-border wire transfers.

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

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

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.

7.2. **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 RE, is intentionally structuring domestic wire transfers below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish identity and if the same transaction is found to be suspicious, STR may be filed with FIU-IND in accordance with the PML Rules.

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

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

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

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

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.

7.3. **Other Obligations**

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

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

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

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

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

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

Bank 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. Bank's responsibility to fulfil record management requirements

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

8. Maintenance of KYC Documents and Preservation of Period

PML Act and Rules cast certain obligations on the banks with regard to maintenance, preservation and reporting of customer account information. Bank shall take all steps considered necessary to ensure compliance with the requirements of the Act and Rules ibid.

8.1 Maintenance of records of transactions

Bank shall maintain all necessary information in respect of transactions prescribed under Rule 3 of PML Rules, 2005 so as to permit reconstruction of individual transactions, including the following information:

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.

8.2 Preservation of Records

Bank shall take appropriate steps to 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.

Bank shall 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 amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

i. Bank shall ensure that records pertaining to the identification of the customers and their address obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended as required under Rule 10 of the Rules ibid.
ii. The identification records and transaction data shall be made available to the competent authorities upon request.
iii. Bank shall maintain records of the identity of clients, and records in respect of transactions with its clients referred to in Rule 3, in hard or soft format.

iv. Evolve a system for proper maintenance and reservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or requested by competent authorities.

v. Bank shall pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background, including all documents / office records / memorandums pertaining to such transactions and purpose thereof shall, as far as possible, be examined and the findings, at branch as well as Principal Officer Level, shall be properly recorded. Such records and related documents shall be made available to help auditors to scrutinize the transactions and also to Reserve Bank / other relevant authorities.

These records will be preserved for five years as is required under PMLA, 2002.

9. Combating Financing of Terrorism (CFT)

The United Nations periodically circulates the following two lists of individuals and entities, suspected of having terrorist links, and as approved by its Security Council (UNSC):

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

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

The United Nations Security Council Resolutions (UNSCRs), received from Government of India, are circulated by the Reserve Bank to all banks and FIs. Bank shall take them into account for implementation of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, **as detailed under para 9.1**.

Branches are required to screen customer names with UN List of terrorist individuals / entities before creation of new CIF / opening of accounts. Branches are required to ensure that the name (s) of the proposed customer does not match with that of the UN list of Terrorist individuals / organization / entities, before opening any new account. AML Cell, Head Office, will also cross check the details of all existing accounts with the updated list, on a daily basis. Branches have to verify transaction and ensure that no account is held by or linked to any of the entities or individuals included in the list maintained for this purpose. If the particulars of any of the account(s) have resemblance with those appearing in the list, bank has to verify transactions carried out in such accounts and report those accounts to RBI / Financial Intelligence Unit-INDIA apart from advising Ministry of Home Affairs as required under UAPA notification dated February 2, 2021.

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

i. The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has issued an Order dated August 27, 2009 detailing the procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 for prevention of, and for coping with terrorist activities. In terms of Section 51A, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by on behalf of or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism and prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

ii. Bank shall strictly follow the procedure laid down in the UAPA revised order dated February 2, 2021, in supersession of the earlier order dated March 14, 2019 (Annex VI of this policy) and ensure meticulous compliance with the Order issued by the Government.

iii. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

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

(a) Bank shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD)
and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated January 30, 2023, by the Ministry of Finance, Government of India (Annex X of this Master Direction).

(b) In accordance with paragraph 3 of the aforementioned Order, bank shall 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 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 FIU-IND 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 CNO.

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

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

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

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

Bank 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.

In addition to the above, bank 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.

9.3 Jurisdictions that do not or insufficiently apply the FATF Recommendations

a) FATF Statements circulated by Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.

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

d) REs are encouraged to leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements.

10. Reporting Requirements

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

Under FATCA and CRS, Bank is required to adhere to the provisions of Income Tax Rules 114F, 114G and 114H as a Reporting Financial Institution as defined in Income Tax Rule 114F.

Roles & responsibilities of Planning Department, NRI Cell

Planning Department NRI Cell, HO is responsible for submission of report to Income Tax Department as per following directions:-

(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. NRI Cell, Planning Department HO is submitting report to Income Tax Department.
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. Bank has appointed Executive Director as Designated Director of the Bank as required to ensure overall 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.
Planning Department, NRI Cell shall take note of the following:

i. updated Guidance Note on FATCA and CRS issued by RBI
ii. a press release on 'Closure of Financial Accounts' under Rule 114H

10.2 Reporting to Financial Intelligence Unit – India

a. In terms of Rule 3 of the PML (Maintenance of Records) Rules, 2005, Bank is required to furnish information relating to cash transactions, cash transactions integrally connected to each other, and all transactions involving receipts by non-profit organisations [NPO means any entity or organisation 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 (erstwhile Section 25 of Companies Act, 1956) Section 8 of the Companies Act, 2013], cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine, cross border wire transfer, etc. to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:
The Director, FIU-IND, Financial Intelligence Unit-India, 6th Floor, Jeevan Bharti Building, Connaught Place New Delhi-110001. Website - http://fiuindia.gov.in/.

b. FIU-IND has released a comprehensive reporting format guide to describe the specifications of prescribed reports to FIU-IND. FIU-IND has also developed a Report Generation Utility and Report Validation Utility to assist reporting entities in the preparation of prescribed reports. The Office Memorandum issued on Reporting Formats under Project
Latest Reporting guide of FIU - IND containing all relevant details are available on FIU's website. **FIU-INDIA in their REPORTING FORMAT GUIDE, informed that for account based transaction, bank shall report in ACCOUNT BASED REPORTING FORMAT (ARF) and whenever transaction without account based relationship with the customer, bank shall report in TRANSACTION BASED REPORT FORMAT (TRF).**

c. In terms of Rule 8, 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 misrepresented transaction beyond the time limit as specified in the Rule shall constitute a separate violation. Branches shall take note of the timeliness of the reporting requirements and submit the reports within the timelines.
As a part of transaction monitoring mechanism, Bank shall put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of the customers. The software shall be robust enough to throw the alerts for effective identification and reporting of suspicious transactions.

As per Rule 7 of PML Rules, the procedure and manner of furnishing information shall be as under:

i. The Bank shall communicate to the Director, FIU-IND the name, designation and address of the Designated Director and the Principal Officer.

ii. The Principal Officer shall furnish the information to the Director on the basis of information available with the reporting entity. A copy of such information shall be retained by the Principal Officer for the purposes of official record.

iii. The Bank shall evolve an internal mechanism having regard to any guidelines issued by regulator, for detecting the transactions referred for furnishing information about such transactions in such form as may be directed by its Regulator.

iv. The Bank, its Designated Director, officers and employees shall observe the procedure and the manner of furnishing information as specified by its Regulator.

10.3 Cash Transaction Reports (CTR)

The Bank shall scrupulously adhere to the following:

- The Cash Transaction Report (CTR) for each month shall be submitted to FIU-IND by 15th of the succeeding month. Bank shall ensure to submit CTR for every month to FIUIND within the prescribed time schedule.
- All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine shall be reported by the Principal Officer of the Bank to FIU-IND in the specified format (Counterfeit Currency Report- CCR) by 15th day of the next month. These cash transactions shall also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.
- While filing CTR, details of individual transactions below Rupees Fifty Thousand need not be furnished.
- CTR shall contain only the transactions carried out by the Bank on behalf of their clients / customers excluding transactions between the internal accounts of the Bank.
- A summary of cash transaction report for the Bank as a whole shall be compiled by the Principal Officer of the Bank every month in physical form as per the format specified. The summary shall be signed by the Principal Officer and submitted to FIU¬IND. In case of Cash Transaction Reports (CTR) compiled centrally by banks for the branches having Core

Banking Solution (CBS) at their central data centre level, banks may generate centralized Cash Transaction Reports (CTR) in respect of branches under Core Banking Solution at one point for onward transmission to FIU-IND, provided the CTR is generated in the format prescribed by FIU-IND.

- A copy of the monthly CTR submitted to FIU-India in respect of the branches shall be available at the Bank for production to auditors / inspectors, when asked for.
- The instruction on 'Maintenance of records of transactions' and 'Preservation of records' as contained at Para 8.1 and 8.2 respectively shall be scrupulously followed by the branches.

10.4 Suspicious Transaction Reports (STR)

i. While determining suspicious transactions, Bank shall be guided by the definition of suspicious transaction as contained in PMLA Rules as amended from time to time.

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

iii. Bank shall make STRs if there is a reasonable ground to believe that the transaction involves proceeds of crime irrespective of the amount of transaction and / or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

iv. The Suspicious Transaction Report (STR) shall be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report shall be made available to the competent authorities on request.

v. In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, branches may consider the indicative list of suspicious activities contained in Annexure-V of this Note.

vi. Bank shall not put any restrictions on operations in the accounts where an STR has been filed. Bank and their employees shall keep the fact of furnishing of STR strictly confidential, as required under PML rules. Moreover, it shall be ensured that there is no tipping off to the customer at any level.

The bank has implemented centralized processing and submission of STRs on the following lines:

AML/CFT Cell, HO shall process the AML alerts generated / reported and escalate suspicious transactions, if any for review and submit the STRs to FIU-IND, Delhi.

10.5 Non-Profit Organizations Report (NTR)

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

10.6 Cross-border Wire Transfer Report (CBWTR)

Cross-border Wire Transfer Report (CWTR) is required to be filed by 15th of succeeding month for all cross-border wire transfers of the value of more than Rupees five lakh or its equivalent in foreign currency where either the origin or destination of fund is in India.

As per recent amendments to Prevention of Money Laundering (PML) Rules, every reporting entity is required to maintain the record of all transactions including the record of all cross border wire transfers of more than Rs. 5 lakh or its equivalent in foreign currency, where either the origin or destination of the fund is in India.

The information shall be furnished electronically in the FIN-Net module developed by FIUIND.

11. General Guidelines

11.1 Confidentiality of customer information

The information collected from the customer for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling etc. Information sought from the customer shall be relevant to the perceived risk and be non-intrusive. Any other information that is sought from the customer shall be called for separately only after the account has been opened, with his/her express consent and in a different form, distinctly separate from the application form. It shall be indicated clearly to the customer that providing such information is optional.

11.2 Secrecy Obligations and Sharing of Information

Bank shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.

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

While considering the requests for data / information from Government and other agencies, Bank shall satisfy itself 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:

a. Where disclosure is under compulsion of law

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

c. the interest of bank requires disclosure and

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

11.3 Avoiding hardship to customers

Branches should keep in mind the spirit of instructions issued by the RBI and avoid undue hardships to individuals who are otherwise classified as low risk customers.

11.4 Sensitizing Customers

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

11.5 Hiring of Employees

KYC norms / AML standards / CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking channels. Therefore, Bank shall put in place adequate screening mechanism as an integral part of its personnel recruitment / hiring process.

Bank shall 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. Bank shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

11.6 Employee Training

Bank shall have an ongoing employee training programme so that the members of the staff are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. Staff /Officials working in AML Cell (Head Office) should complete AML-KYC Certification course from IIBF mandatorily.

The front desk staff needs to be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the Bank, regulation and related issues shall be ensured.

11.6 Accounts under Foreign Contribution Regulation Act, 2010 (FCRA)

RBI vide letter no:DOR.AML.No.1783/14.08.001/2020-21 dated December 09, 2020.RBI has informed that Ministry of Home Affairs (MHA), Government of India has issued gazette notification regarding the Foreign Contribution (Regulation) Amendment Act, 2020, The said amendment Act has been notified on September 28, 2020 and has been enforced from September 29, 2020 through notification of date

In terms of the amended Section 17 of the above-mentioned amendment act, every person/ NGO/ association who have been granted FCRA certificate of registration under FCRA 2010 and prior permission to receive foreign contribution shall henceforth receive such contribution only in an account designated as "FCRA Account" **in the specified branch (Main Branch) of State Bank of India (SBI) at New Delhi**. No person/ NGO/ association shall receive foreign contributions received in accordance with the FCRA 2010 in any account other than the one designated as "FCRA Account" as per section 17(1) of the FCRA Act, 2010 in the specified branch, i.e., **New Delhi Main Branch of the SBI, Sansad Marg, New Delhi**, post opening of such an account.

In terms of section 46 of the Foreign Contribution (Regulation) Act, 2010, **the MHA has advised to instruct all the scheduled banks to stop receiving/ crediting with effect from April 01, 2021 any foreign contributions in any account other than the "designated FCRA Account**" in the aforesaid branch of the SBI at New Delhi, which has been opened by the person who has been granted certificate or prior permission under the FCRA, 2010. **The period from September 29, 2020 till March 31, 2021 will be treated as transition period to facilitate opening of the designated "FCRA Account**".

MHA has also clarified that the person/ NGO/ association would be free to retain their present account as "other FCRA Account" in any branch of a scheduled bank of their choice which they can link with the "designated FCRA Account" opened in the SBI, New Delhi Main Branch as specified by the Central Government. All foreign contributions shall be received only in the "designated FCRA Account" with the SBI from the date of opening of such account or April 01, 2021, whichever is earlier.

All branches and offices to **strict adherence to above guidelines of RBI**. The standard operating procedure for opening FCRA Account at the SBI, New Delhi Main Branch is available on the website:

https://bank.sbi/documents/16012/1557541/20112020_SOP+for+FCRA+Accounts.pdf/e473a6d3-51b8-6da1-c5af-add2a0e4287d?t=1605875107975

11.8 Technology requirements

The AML software in use at the Bank shall be comprehensive and robust enough to capture all cash and other transactions, including those relating to walk-in customers, sale of gold / silver / platinum, payment of dues of credit cards / reloading of prepaid / travel cards, third party products, and transactions involving internal accounts of the Bank.

ANNEX – I

Digital KYC Process

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

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

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

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

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

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

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

H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead

of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/eAadhaar.

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

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

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

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

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

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

(iii) All of the necessary details in CAF including mandatory field are filled properly; On Successful verification, the CAF shall be digitally signed by authorized officer of the bank who will take a print of CAF, get signatures / thumb impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

ANNEX – II

Customer Identification Procedure-Features to be verified and Documents that may be obtained from Customers:

Feature	Documents
Accounts of Individuals	
Proof of Identity and Address	For undertaking Customer Due Diligence (CDD), bank shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity. **A.** Aadhaar Number where, ❖ the customer is desirous of receiving any benefit or subsidy, benefit or service for which the expenditure is incurred from, under any scheme notified by Central Government or State Government; or ❖ the customer decides to submit his Aadhaar number voluntarily to a bank without consultation with the Unique Identification Authority of India; or **B.** The proof of possession of Aadhaar number where offline verification can be carried out; or **C.** The proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; **D.** The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income tax Rules, 1962; and **E.** Such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the bank. Provided that where the customer has submitted, (i) Aadhaar number under clause (A) above, branch shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India. Further, in such case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the bank.

Feature	Documents
	(ii) Proof of possession of Aadhaar under clause (B) above where offline verification can be carried out, the bank shall carry out offline verification. (iii) An equivalent e-document of any OVD, the bank shall verify the digital signature and take a live photo. (iv) Any OVD or proof of possession of Aadhaar number under clause (C) above where offline verification cannot be carried out, the bank shall carry out verification through digital KYC. Provided that for a period not beyond such date as may be notified by the Government for a class of Bank, instead of carrying out digital KYC, the Bank pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent e- document is not submitted. **Officially Valid Documents (OVD) are as under:** ❖ **Proof of Possession of Aadhaar Number** ❖ **Passport** ❖ **Driving License** ❖ **Voter's Identity Card issued by Election Commission of India** ❖ **Job Card issued by NREGA duly signed by an officer of the State Government** ❖ **Letter issued by the National Population Register containing details of name and address** ❖ **Any other document as notified by the Central Government in consultation with the Regulator.**
Accounts of Proprietorship Concerns	
Proof of name, address and activity of the concern	For Proprietary concerns, Customer Due Diligence of the individual (proprietor) are to be carried out and any two of the following documents or the equivalent e-documents in the name of the proprietary concern should be submitted: i. Registration certificate (in the case of a registered concern). ii. Certificate / license issued by the Municipal authorities under Shop and Establishment Act. iii. Sales and income tax returns. iv. CST/VAT/ GST certificate (provisional / final). v. Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities. vi. 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.

Feature	Documents
	vii. Utility bills such as electricity, water, landline telephone bills, etc viii. 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. Though the default rule is that any two documents mentioned above should be provided as activity proof by a Proprietary concern, in cases where the branches are satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the branches, however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern. **For opening of current account-Need for discipline refer bank circular AX1/CrMon/CA/19/2021-22 dated 30.10.2021 and SOP in this regard.** Credit facility would include Term Loans, Overdraft, Cash Credit, Working Capital Limits, Bank Guarantee, Letter of Credit, Export Finance, Mortgage Loans, Warehouse Receipt Finance, Factoring, Bill Discounting, Cheque Discounting, Import Finance (Buyer's Credit), Treasury Limits or any other limit either secured or unsecured.
Accounts of Partnership Firms	
	Where the customer is a partnership firm, certified copies of following documents or the equivalent e-documents of all the following documents are to be submitted: i. Registration Certificate ii. Partnership Deed iii. Permanent Account Number of the Partnership Firm iv. Any Officially Valid Document which contains proof of identity and address, one recent photograph and Permanent Account No or Form 60/61 of related **beneficial owner**, managers, officers or employees, as the case may be, holding an attorney to transacts on its behalf. **For opening of current account-Need for discipline refer bank circular AX1/CrMon/CA/19/2021-22 dated 30.10.2021 and SOP in this regard** Credit facility would include Term Loans, Overdraft, Cash Credit, Working Capital Limits, Bank Guarantee, Letter of Credit, Export Finance, Mortgage Loans, Warehouse Receipt Finance, Factoring, Bill Discounting, Cheque Discounting, Import Finance (Buyer's Credit), Treasury Limits or any other limit either secured or unsecured.

Feature	Documents
Accounts of Companies	
	Where the customer is a company, certified copies of documents or the equivalent e-documents of all the following documents are to be submitted: i. Certificate of incorporation ii. Memorandum and Articles of Association iii. Permanent Account Number of the Company iv. A resolution from the Board of Directors and Power of Attorney granted to its managers, officers or employees to transact on its behalf. v. Any Officially Valid Document containing proof of identity and address, one recent photograph and Permanent Account Number or Form 60/61 of related **beneficial owner**, managers, officers and employees, as the case may be, holding an attorney to transact on its behalf. **For opening of current account-Need for discipline refer bank circular No.- AX1/CrMon/CA/19/2021-22 dated 30.10.2021 and SOP in this regard**. Credit facility would include Term Loans, Overdraft, Cash Credit, Working Capital Limits, Bank Guarantee, Letter of Credit, Export Finance, Mortgage Loans, Warehouse Receipt Finance, Factoring, Bill Discounting, Cheque Discounting, Import Finance (Buyer's Credit), Treasury Limits or any other limit either secured or unsecured.
Accounts of Limited Liability Partnership (LLP)	
	i. Certified copy of incorporation documents filed with the registrar companies. ii. Certificate issued by the registrar of the companies iii. Copy of LLP Agreement signed by all the partners. In case, there is no LLP agreement, schedule I of LLP Act signed by all the partners will prevail. iv. Any Officially Valid Document which contains proof of identity and address in respect of person holding an attorney to transacts on its behalf and v. Permanent Account Number or Form 60/61 as defined in the Income Tax Rules, 1962 issued to the person holding a power of Attorney to transact on its behalf.
Accounts of Trusts	

Feature	Documents
	Where the customer is a Trust, certified copies of documents or the equivalent e-documents of all the following documents are to be submitted: i. Registration Certificate ii. Trust Deed iii. Permanent Account Number or Form 60/61 of the Trust iv. Any Certified Officially Valid Document which contains proof of identity / address, one recent photograph and Permanent Account Number of Form 60/61 of the related **beneficial owner**, managers, officers or employees holding an attorney to transact on its behalf.
Accounts of Unincorporated Association or Body of Individuals	
	Where the customer is an unincorporated association or a body of individuals, certified copies of documents or the equivalent e-documents of all the following documents are to be submitted: i. Resolution of the managing body of such association or body of individuals. ii. Permanent Account Number or Form 60/61 of the Unincorporated association or a body of individuals. iii. Power of Attorney granted to the person who will transact on its behalf. iv. Any Certified Officially Valid Document containing proof of identity and address, one recent photograph and Permanent Account Numbers of Form 60/61 of the person, beneficial owner, managers, officers or employees holding an attorney to transact on its behalf.
Accounts of Governments or its Departments, Societies, Universities and Local Bodies like village panchayats	
	The certified copies of the following documents or the equivalent e-documents thereof are to be submitted: i. Document showing name of the person authorized to act on behalf of the entity; ii. Any Certified Officially Valid Document which contains proof of identity / address in respects of managers, officers and employees holding an attorney to transacts on its behalf. iii. PAN or Form 60/61 as defined in the Income Tax Rules, 1962 issued to the person holding an attorney to transact on behalf of the entity. iv. Such documents as may be required to establish the legal existence of such an entity / juridical person

Feature	Documents
Branches to obtain only the documents as mentioned above and not to accept any other document for KYC purpose.	

ANNEX – III

List of Low / Medium / High risk Customers based on the recommendations of IBA Working Group.

APPENDIX – A

Low Risk	Medium Risk	High Risk
- Cooperative Bank - Ex-staff, Govt. / Semi Govt. Employees - Illiterate Individual - Local Authority - Other Banks Pensioner - Public Ltd. - Public Sector - Public Sector Bank Staff - Regional Rural Banks - Govt./Semi Govt. - Local Body - Senior Citizens - Self Help Groups	- Gas Station - Car / Boat / Plane Dealership - Electronics (wholesale) - Travel agency - Used car sales - Telemarketers - Providers of telecommunications service, internet cafe, IDD call service, phone cards, phone center - Dot-com company or internet business - Pawnshops - Auctioneers - Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores. - movie theaters, etc. - Sole Practitioners or Law Firms (small, little known). - Notaries (small, little known) . - Secretarial Firms (small, little known) - Accountants (small, little known firms) - Venture capital companies - Blind - Purdanashin - Registered Body - Corporate Body	- Individuals entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc. - 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 - Individuals and entities in watch lists issued by Interpol and other similar internationals organizations. - Customers with dubious reputation as per public information available or commercially available watch lists Individual and entities specifically identified by regulators, FIU and other competent authorities as high-risk 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. Customers based in high risk Countries / jurisdictions or locations (refer Appendix C) - Politically exposed persons (PEPs) of foreign origin, Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;

	- Joint Sector partnership	- Non-resident Customer - Embassies / Consulates - Off-shore (foreign) corporation / business - Non face-to-face Customers - High net worth individuals - Firms with 'sleeping partners' - Companies having close family shareholding or beneficial ownership - Complex business ownership - Structures, which can make it easier to conceal underlying beneficiaries, where there is legitimate commercial rationale. - Shell companies which have no physical presence companies in the country in which it is incorporated. The existing simply of a local agent or low level staff does not constitute physical presence - Investment Management / Money Management Company / Personal - Investment Company - Customer Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc. - Trusts, charities, NGOs / NPOs (especially those operating on a “cross border” basis) unregulated clubs and organisations receiving donations (excluding NPOs / NGOs promoted by - United Nations or its agencies) - Money Service Business: including seller of: Money Orders / Travelers‘ Cheques / Money Transmission / Cheque Cashing / Currency Dealing or Exchange - Business accepting third party cheques (except supermarkets or retail stores that accept payroll cheques / cash payroll cheques) - Gambling / gaming including “Junket Operators” arranging gambling tours - 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) - Customers engaged in a business which is associated with higher levels of corruption (e.g. Arms manufacturers, dealers and intermediaries) - Customers engaged in industries that might relate to nuclear proliferation activities or explosives - Customers that may appear to be Multilevel marketing companies etc. - Customers dealing in Real Estate business (transactions need to be monitored with enhanced due diligence) - Associations/Clubs - Foreign Nationals - NGO - Overseas Corporate Bodies - Bullion dealers and jewellers (subject to enhanced due diligence) - Pooled accounts - Other Cash Intensive business - Shell Banks - Transactions in corresponding banking - Non-Bank Financial Institution - Stock brokerage - Import / Export - Executors/Administrators - HUF - Minor Accounts under Foreign Contribution Regulation Act

The above categorization of customers under risk perception is only illustrative and not exhaustive.	
Updating KYC of low risk customers:	Every 10 years.
Updating KYC of medium risk customers:	Every 8 years
Updating KYC of high-risk customers:	Every 2 years

APPENDIX – B

High / Medium Risk Products and Services

Branches / Offices are required to pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Presently a variety of Electronic Cards are used by customers for buying goods and services, drawing cash from ATMs, and for electronic transfer of funds. Branches should ensure that appropriate KYC procedures are duly applied before issuing the Cards including Add-on / Supplementary Cards to the customers

Indicative list of High / Medium Risk Products and Services

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

APPENDIX – C

High / Medium Risk Geographic risk

Branches / offices are required to prepare a profile for all new customers based on risk categorization, taking into account the location of the customer and the customer's clients as well as factors such as the nature of business activity, mode of payments, turnover and customer's social and financial status including location of his business activity and to exercise due diligence based on the bank's risk perception. The customer should be subjected to higher due diligence if following criteria falls under "high-risk" geographies

- Country of nationality (individuals)
- Country of residential address (individuals)
- Country of incorporation (legal entities)
- Country of residence of principal shareholders / beneficial owners (legal entities)
- Country of business registration such as branch / liaison / project office
- Country of source of funds
- Country of the business or correspondence address
- Country with whom customer deals (e.g. 50% of business – trade, etc.)

Apart from the risk categorization of the countries, branches / offices should categorize the geographies / locations within the country on both Money Laundering (ML) and Financing Terrorism (FT) risk.

Indicative List of High / Medium Risk Geographies

A. Countries / Jurisdictions

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

B. Locations

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

High risk countries / jurisdictions or locations			
Iran	Albania	Kuwait	Sudan

Democratic People's Republic of Korea (DPRK)	Angola	Lao PDR	Syria
Algeria	Argentina	Namibia	Tajikistan
Ecuador	Cambodia	Nicaragua	Turkey
Indonesia	Cuba	Pakistan	Uganda
Myanmar	Ethiopia	Panama	Yemen
Afghanistan	Iraq	Papua New Guinea	Zimbabwe

NOTE:

Risk assessment should take into account following risk variables specific to a particular customer or transaction:

- The purpose of an account or relationship
- Level of assets to be deposited by a particular customer or the size of transaction undertaken.
- Level of regulation or other oversight or governance regime to which a customer is subjected to.
- The regularity or duration of the relationship.
- Familiarity with a country, including knowledge of local laws, regulations and rules as well as structure and extent of regulatory oversight.
- The use of intermediate corporate vehicles or other structures that have no apparent commercial or other rationale or increase the complexity or otherwise result in lack of transparency

ANNEX – IV

Monitoring / Review of Customer Risk Categorization (CRC)

Customer Behavior Indicators which may lead to migration of Risk categorization to "High Risk" are as follows:

- Customers who are reluctant in providing normal information while opening an account, providing minimal or fictitious information or when applying to open an account, providing information that is difficult or expensive for the Bank to verify.
- Customer expressing unusual curiosity about secrecy of information involved in the transaction.
- Customers who decline to provide information that in normal circumstance would make the customers eligible for banking services.
- Customer giving confusing details about a transaction.
- Customer reluctant or refuses to state a purpose of a particular large / complex transaction / source of funds involved or provides a questionable purpose and / or source.
- Customers who use separate tellers to conduct cash transactions or foreign exchange transactions.
- Customers who deposit cash / withdrawals by means of numerous deposit slips / cheques leaves so that the total of each deposit is unremarkable, but the total of all credits / debits is significant.
- Customers' representatives avoiding contact with the branch.
- Customer who repays the problem loans unexpectedly.
- Customers who appear to have accounts with several banks within the same locality without any apparent logical reason.
- Customer seeks to change or cancel a transaction after the customer is informed of currency transaction reporting / information verification or record keeping requirements relevant to the transaction.
- Customers regularly issue large value cheques without balance and then deposits cash.
- Sudden transfer of funds from unrelated accounts through internet (or such other electronic channels) and subsequent quick withdrawal through ATM.

A. Transactions involving large amounts of cash

- Exchanging an unusually large amount of small denomination notes for those of higher denomination.
- Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank.
- Frequent withdrawal of large amounts by means of cheques, including traveler's cheques.
- Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity.
- Large cash withdrawals from a previously dormant / inactive account, or from an account which has just received an unexpected large credit from abroad.

- 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.
- 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.

B. Transactions that do not make Economic Sense

- Customer having multiple accounts with the bank, with frequent transfers between different accounts.
- Transactions in which amounts are withdrawn immediately after being deposited, unless the customer‘s business activities furnish plausible reasons for immediate withdrawal.

C. Activities not consistent with the customer’s business

- Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.
- 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 the corporate business activity / dealings.
- Unusual applications for DD / PO / NEFT/ RTGS against cash.
- Accounts with large volume of credits through DD / PO / NEFT / RTGS whereas the nature of business does not justify such credits.
- Retail deposit of many cheques but rare withdrawals for daily operations.

D. Attempts to avoid reporting / record- keep requirements

- 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.
- Any individual or group that coerces / induces or attempts to coerce/ induce a bank employee not to file any reports or any other forms.
- 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 customers intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

E. Unusual Activities

- An account of a customer who does not reside / have office near the branch even though there are bank branches near his residence / office.
- A customer who often visits the safe deposit area immediately before making cash deposits, especially deposits just under the threshold level.
- Funds coming from the list of countries / centres, which are known for money laundering.

F. Customer who provides insufficient or suspicious information

- 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.

- A customer / company who is reluctant to reveal details about his/its activities or to provide financial statements
- A customer who has no record of past or present employment but makes frequent large transactions.

G. Certain suspicious funds transfer activities

- Sending or receiving frequent or large volumes of remittances to/from countries outside India.
- Receiving large DD/ NEFT/ RTGS remittances from various centres and remitting the consolidated amount to a different account / centre on the same day leaving a minimum balance in the account.
- Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire / fund transfer.

H. Bank no longer knows the true identity

When a bank believes that it would no longer be satisfied that it knows the true identity of the account holder.

I. Some examples of suspicious activities / transactions to be monitored by the operating staff

- Large Cash Transactions
- Multiple accounts under the same name
- Frequently converting large amounts of currency from small to large denomination notes
- Placing funds in term Deposits and using them as security for more loans large deposits immediately followed by wire transfers.
- Sudden surge in activity level.
- Same funds being moved repeatedly among several accounts.
- Multiple deposits of money orders, Banker's cheques, drafts of third Parties Multiple deposits of Banker's cheques, demand drafts, cross / bearer.
- Cheques of third parties into the account followed by immediate cash withdrawals.
- Transactions inconsistent with the purpose of the account.
- Maintaining a low or overdrawn balance with high activity

J. Check list for preventing money-laundering activities

- A customer maintains multiple accounts, transfers 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).

- 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 money.
- 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.
- 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.
- A customer experiences increased wire activity when previously there has been no regular wire activity.
- Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.
- A business customer uses or evidences or sudden increase in wire transfer to send and receive large amounts of money, internationally and/ or domestically and such transfers are not consistent with the customer's history.
- 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.
- Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.
  - Instructing the Bank to transfer funds abroad and to expect an equal incoming wire Transfer from other sources.
- Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency
- Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.
- Periodic wire transfers from a person's account (s) to Bank haven countries.
- A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.
- 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 travelers' cheques.
- 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. 10 Lakh).
  a. The amount is just under a specified threshold.
  b. The funds come from a foreign country or
  c. Such transactions occur repeatedly.
- A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Bankers' cheques (just under a specified threshold).
- A Non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit

ANNEX – V

KYC documents for eligible FPIs under PIS

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

			FPI Type	
Document Type		**Category I**	**Category II**	**Category III**
		given in case of PoA to Global Custodian	given in case of PoA to Global Custodian	
	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *
Ultimate Beneficial Owner (UBO)	List	Exempted *	Mandatory (can declare "no UBO over 25%")	Mandatory
	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *

*Not required while opening the bank account. However, FPIs concerned may submit an undertaking that upon demand by Regulators/Law Enforcement Agencies the relative document/s would be submitted to the bank.

@ FPIs from certain jurisdictions where the practice of passing Board Resolution for the purpose of opening bank accounts etc. is not in vogue, may submit 'Power of Attorney granted to Global Custodian/Local Custodian In lieu of Board Resolution'

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

ANNEX – VI

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".

In order to ensure expeditious and effective implementation of the provisions of Section 51A, a revised procedure of orders and guidelines on the subject:

1. Communication details of the UAPA Nodal Officers:

The Additional Secretary (CTCR), Ministry of Home Affairs, would be the Central [designated] Nodal Officer for the UAPA at Fax No. 011-230923465 and also convey over telephone on 011-23092456. The particulars apart from being sent by post should necessarily be conveyed on e-mail **jsctcr-mha@gov.in.**

2. Communication of the list of designated individuals / entities

a. 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.

b. The Financial Regulators shall forward the list of designated persons as mentioned in Para 2.1 above, without delay to the banks, stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies.

c. The Central Nodal Officer for the UAPA shall forward the designated list as mentioned in Para 2.1 above, to all the UAPA Nodal Officers of States/UTs without delay.

d. The UAPA Nodal Officer in Foreigners Division of MHA shall forward the designated list as mentioned in Para 2.1 above, 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.

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

i. To maintain updated designated lists in electronic form and run a check on the given parameters on a daily basis to verify whether individuals or entities listed in the Schedule to the Order, hereinafter, referred to as designated individuals / entities are holding any funds, financial assets or economic resources or related services held in the form of bank accounts, stocks, Insurance policies etc., with them.

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

iii. The banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall also send a copy of the communication mentioned in 3.1 (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 Nodal Officer for the UAPA at Fax No. 011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsctcr-mha@gov.in, without delay.

v. The banks, stock exchanges / depositories, intermediaries regulated by SEBI, and insurance companies shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts, covered under Paragraph 3.1(ii) above, carried through or attempted as per the prescribed format.

b. On receipt of the particulars, as referred to in Paragraph 3 (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.

c. 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.

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

a. 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.

b. 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.

c. 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.

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

e. 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.

f. 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.

5. Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001.

a. 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.

b. 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.

c. 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. **6. 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 3 and 4 above shall be followed**.

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

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

a. 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;

b. The addition may be allowed to accounts of the designated individuals/ entities subject to the provisions of paragraph 7 of:

a. interest or other earnings due on those accounts, or

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

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

8. Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person:

a. 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, Registrar of Immovable Properties and the State/UT nodal officers.

b. The banks, Registrar of Immovable Properties 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 nodal officer of **CTCR** Division of MHA as per the contact details given in paragraph 1(ii) above within two working days.

c. 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.

9. Regarding prevention of entry into or transit through India

a. As regards prevention of entry into or transit through India of the designated individuals, 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.

b. The immigration authorities shall ensure strict compliance of the Orders and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the Foreigners' Division of MHA.

10. Procedure for communication of compliance of action taken under Section 51 A.

The Central Nodal Officers for the UAPA and the Nodal Officer in the Foreigners Division of 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.

11. Communication of Order issued under Section 51A of Unlawful Activities (Prevention) Act, 1967:

All Orders under section 51A of Unlawful Activities (Prevention) Act, 1967 relating to funds, financial assets or economic resources or related services, shall be communicated to all banks, Regulators of Financial Services, FIU-IND and DNFBPs, depositories / stock exchanges, intermediaries regulated by SEBI, Registrars performing the work of registering immovable properties, through the UAPA nodal officer of the State/UT

END