Policy Guidelines on KYC/AML/CFT-2020-21.

1. INTRODUCTION

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

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

1.3 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, including operational instructions issued in pursuance of such amendment(s).

1.4 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.

1.5 This policy has been compiled covering the guidelines issued by RBI/GOI up to January 2020.

2. OBJECTIVES OF THE POLICY

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

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

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

3. SCOPE OF THE POLICY

3.1 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.

3.2 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

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

4.2 Definition of 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.

4.3 Definition of Central KYC Records Registry

"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.

4.4 Definition of Customer Due Diligence (CDD)

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

4.5 Beneficial Owner (BO)

Rule 9(3) of the Prevention of Money Laundering Rules, 2005 requires that every banking company, and financial institution, as the case may be, shall identify the beneficial owner and take all reasonable steps to verify his identity. The term "Beneficial Owner" has been defined as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person.

A juridical person is an Entity that is not a single natural person (as a human being), authorized by law with duties and rights, recognized as a legal authority having a distinct identity, a legal personality (Also known as artificial person, juridical entity, juristic person, or legal person).

The procedure for determination of Beneficial Ownership as per RBI/Government guidelines is as under:

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

Explanation - For the purpose of this sub-clause-

a. "Controlling ownership interest" means ownership of or entitlement to more than twenty-five percent of shares or capital or profits of the company;

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

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

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

d) where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

e) where the **client is a trust,** the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

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

There exists the possibility that trust / nominee or fiduciary accounts can be used to circumvent the customer identification procedures. In such cases, Bank shall determine whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary. If so, Bank shall insist on satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. The different categories of beneficiaries should be identified as defined above. In the case of a 'foundation', steps shall be taken to verify the founder managers / directors and the beneficiaries, if defined.

4.6 Definition of Adhaar 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).

4.7 Definition of Authentication

"Authentication", in the context of Aadhaar authentication, means the process as 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.

4.8 Definition of 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 which can access at https://digitallocker.gov.in/.

Equivalent e-document has also been permitted for accounts of non-individual customers.

4.9 Definition of Officially Valid Documents (OVDs)

4.9.1 "Officially Valid Document" (OVD) means the

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

   Provided that,

   - 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.

4.9.2 For the limited purpose of proof of address the following documents or equivalent e-document thereof shall be deemed to be OVDs:-

a. Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
b. Property or Municipal tax receipt;
c. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
d. Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation;

4.9.3 Where the OVD furnished by the customer does not have updated address, the customer shall submit OVD with current address within a period of three months of submitting the documents specified above 4.10.2.

4.9.4 In respect of joint account holder, for verifying the identity of the customer and proof of address documents or equivalent e-document thereof specified above at 4.10.1 and 4.10.2 shall be deemed to be OVDs.

4.9.5 Further, In respect of foreign national, 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.

4.10 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 authorised 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:

i. Authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
ii. branches of overseas banks with whom Indian banks have relationships,
iii. Notary Public abroad,
iv. Court Magistrate,
v. Judge,
vi. Indian Embassy/Consulate General in the country where the nonresident customer resides.

4.11 Definition of Offline Verification

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 agency must

(i) Obtain the consent of the individual,
(ii) Inform them of alternatives to sharing information, and
(iii) Not collect, use or store Aadhaar number or biometric information.

4.12 Definition of Digital KYC

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

4.13 Definition of 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

1. Any sender may authenticate an electronic record by affixing his digital signature
2. 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—

   a. To derive or reconstruct the original electronic record from the hash result produced by the algorithm;
   b. That two electronic records can produce the same hash result using the algorithm.
3. Any person by the use of a public key of the sender can verify the electronic record.
4. The private key and the public key are unique to the sender and constitute a functioning key pair

4.14 Definition of Know Your Client (KYC) Identifier

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

4.15 Video based Customer Identification Process (V-CIP)

"Video based Customer Identification Process (V-CIP)" is treated like face-to-face method of customer identification by an official of the branch by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information furnished by the customer.

4.16 Definition of Non-Profit Organisations (NPO)

"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 Section 8 of the Companies Act, 2013

4.17 Definition of Non Face to Face Customers

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

4.18 Definition of 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.

4.19 Definition of 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.

4.20 Definition of 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; or
f. Establishing or creating a legal person or legal arrangement.

4.21 Definition of 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.

5. KEY ELEMENTS OF KYC POLICY

The KYC Policy includes the following four key elements:

- Customer Acceptance Policy;
- Customer Identification Procedures (CIP);
- Risk Management and
- Monitoring of Transactions

5.1 Customer Acceptance Policy (CAP)

Bank's Customer Acceptance policy (CAP) lays down the criteria for acceptance of customers. The guidelines in respect of the customer relationship in the Bank broadly are:

1. No account is opened or maintained in anonymous or fictitious / benami name.
2. 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.

3. Branch obtain Permanent Account Number (PAN) and the same shall be verified from the verification facility of the issuing authority.
4. Through digital signature branch shall verify an equivalent e-document which is obtained from the customer as explained in 4.15 in this policy.
5. No transaction or account-based relationship is undertaken without following the CDD procedure.
6. Branches are not required to obtain fresh documents of customers when existing KYC compliant customer approach and desires to open another account with the same branch.
7. While opening a joint account, CDD Procedure is followed for all the joint account holders.
8. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
9. Optional/additional information, is obtained with the explicit consent of the customer after the account is opened.
10. Parameters of risk perception are clearly defined in terms of the nature of business activity, location of the customer and his clients, mode of payments, volume of turnover, social and financial status, etc. so as to enable the Bank in categorizing the customers into low, medium and high risk ones, as detailed in para 5.1.2;
11. 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.
12. 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.
13. 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 Code (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-de-duplication" 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 pre-paid instruments / purchasers of third party products. However, UCIC shall be allotted to such walk-in customers who have frequent transactions in branch.

5.1.2 Risk Perception in respect of Customer

'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 the risk perceptions associated with the parameters comprising a customer's profile, and the risk associated with the product and channel being used by him.

For effective implementation of KYC, anti-money laundering (AML) and combating of financing of terrorism (CFT) measures, Risk Categorization of customers along with compilation, periodic updation of customer profile and monitoring in accounts by banks are very important. Bank become vulnerable to operational risk in case there is weakness in the KYC/AML process. The main goal of risk management is to avoid unfavorable surprise. List of identified risks is required for this. Risks are grouped under a common area which provides a structured & systematic approach for identifying risks.

Customer Risk Categorisation

For categorizing a customer as Low Risk, Medium Risk and High Risk, the parameters considered are customer's identity, social/financial status, nature of business activity, mode of payments, volume of turnover, information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

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.

Medium Risk Customers

Customers who are likely to pose a higher than average risk to the Bank should be categorised 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 client profile, etc. besides proper identification.

The following customers are classified as **Medium Risk Customers**:

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

Updating KYC of Medium Risk Customers : Every 8 years.

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 client 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.

*** Parameters defining High Net worth Individuals (HNIs)**

As per **Meeting of Committee of General Managers** vide letter No **AX1/PLN/KYC/Risk Cat/2019-20 dated 08/05/2019** it has been decided that customers with any of the following shall be treated as High Net worth Individuals;

Average balance exceeding Rs. 25 lakh in SB.
Average Balance exceeding Rs. 50 lakh in CA.
Term deposits exceeding Rs. 50 lakh in aggregate.

Annual turnover exceeding Rs. 25 lakh in the SB account, and exceeding Rs. 100 lakh 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 lakh and above in all deposit accounts (SB+CA+TD).
Enjoying Fund based limits/term loans exceeding Rs. 100 lakh.

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 from system. Once the parameters are finalized, Bank may choose the appropriate risk rating/scoring models by giving due weightage to each parameter as discussed above.

Bank has adopted combination of manual and automatic classification. Based on system generated risk categorisation on the basis of data fields, bank shall finalise 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 (**Annexure III**).
Branches shall prepare a Risk profile of each customer and apply enhanced due diligence measures on High Risk customers. IBA has provided an indicative list of High/Medium Risk Products, Services, Geographies, Locations, etc., for Risk Based Transaction Monitoring by Banks (detailed in Annexure IV in this Policy).

For illustrative examples of Low, Medium and High Risk customers refer Annexure V. 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. For instance, a salary class individual who is generally to be classified under low risk category may be classified otherwise based on the perception of the Branch/Office.

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:

1. **Customer Constitution:** Individual, Proprietorship, Partnership, Private Ltd. etc.
2. **Business Segment:** Retail, Corporate etc.
3. **Country of residence / Nationality:** Whether India or any overseas location / Indian or foreign national.
4. **Product Subscription:** Salary account, NRI products etc.
5. **Economic Profile:** HNI, Public Ltd. Company etc.
6. **Account Status:** Active, inoperative, dormant.
7. **Account Vintage:** Less than six months old etc.
8. Presence in regulatory negative / PEP / Defaulters / Fraudster lists.
9. Suspicious Transaction Report (STR) filed for the customer.
10. 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 categorisation of customers shall be undertake 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.

Risk rating of Customers:

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 client profile etc.

A. 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.

B. Risk Categorisation 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 / behavior (given as **Annexure IV** – Monitoring of Customer Risk Categorisation (CRC).
    - Submitted Suspicious Transaction Reports (STR) for Customer.
    - Submitted Cash Transaction Report (CTR).
    - Frequent Cheque returns.
    - Minors
C. Risk Categorisation 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 (low 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". (**Annexure VIII**)

Risk categorization of Customers undertaken by the Bank

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

- Customer type
- Customer profession.
- Type of business.
- Product code.
- Account status
- Account vintage.
- 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 categorised 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 categorising 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 Categorisation Matrix. Branches are advised to categorise 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 categorised as High Risk. As per RBI directions, Blocked account status should be part of the initial categorisation of an account at the branch level rather than being part of the review of risk categorisation at the central level. Hence, branches are advised to categorise 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 categorised under "High Risk".
Under vintage parameter, newly opened CASA accounts which have not completed 6 months shall be categorised 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 categorisation matrix, such accounts are to be categorised basing on the highest risk category allotted under those parameters.

5.1.3 Roles & Responsibilities

a. Principal Officer

Bank has appointed General Manager, Inspection and Audit, Head office as a 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 KYC/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 KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made there under, as amended from time to time.

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

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

The Principal Officer under PML Act, 2002 shall be the competent authority for fixing the thresholds for generation of AML alerts and the periodicity of reviewing the alerts shall be at half yearly intervals or as and when required.

b. Designated Director

Designated Director means a person designated by the reporting entity (bank, financial institutions, etc. to ensure overall compliance with the obligations imposed and the Rules and includes the managing Director or a whole time

Director duly authorised by the Board of Directors if the reporting entity is a Company.

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.

If the Designated Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may –

- issue a warning in writing; or
- direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or
- direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or
- By an order, levy a fine on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure.

c. <u>PMO, IT Department, H.O</u>

i. IT Department, shall identify the parameters available in the system for risk categorization through the system as per the model suggested in the policy.

ii. PMO Shall review fixing of parameters available through the system half yearly.

iii. 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.

d. <u>AML cell, Inspection & Audit Department H. O.</u>

i. Shall review and provide necessary recommendations/directions to strengthen adherence of KYC/AML guidelines.

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

iii. HO AML cell is responsible for scrutiny / closure of STR alerts and submission of CTR/NTR/CBWTR/CCR/STR to FIU-IND, attending matters raised by FIU-IND, Enforcement Directorate and other enforcing agencies, correspondent banking questionnaires and reporting to Top-Management/Board.

e. <u>Roles and responsibilities of Zonal Offices</u>

- Shall monitor/follow-up process of review/classification/re-classification of Customer Risk Categorisation.
- Shall ensure compliance of Risk Categorization at branches every six months.

- Shall submit periodical reports on implementation/review of risk categorisation to Head Office.
- Shall attend/follow-up audit observations/remarks.

f. Roles and responsibilities of Branches:

- Branches are responsible for ensuring compliances of KYC.
- Branches may also apply additional alert indicators to address specific risks faced by them.

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

Monitoring/Review of Customer Risk Categorisation (CRC)

Branches shall carry out a review of risk categorization of customers at a periodicity of not less than once in six months i.e., as on 15th of May and November every year. During such review, the risk assigned to an existing customer may undergo change depending on the change in risk parameters of the customer.

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

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 could be:

- Customer locations.
- Financial Status.
- Nature of business.
- Purpose of transaction.

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

5.2 Customer Identification Procedure (CIP)

5.2.1 General

i) Customer identification means undertaking Customer Due Diligence (CDD) measures while commencing an account-based relationship including identifying and verifying the customer and the beneficial owner on the basis of one of the OVDs.

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.).

ii) Bank shall have a policy approved by the Board which clearly spells out the Customer Identification Procedure to be carried out at different stages, i.e.

- While establishing a banking relationship;

- While carrying out a financial transaction;
- When the Bank has a doubt about the authenticity or adequacy of the customer identification data it has obtained;
- When bank sells third party products as agent;
- 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/-
- 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;
- 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/-.
- While opening accounts bank ensure that introduction is not to be sought.
- Due diligence of the customer carried out by the third party, records or the information is obtained from the third party or from the Central KYC Records Registry within two days.
- At the time of opening the account / during periodic updation, 'Mandatory' information required for KYC purpose customer is obliged to give while opening an account should be obtained.
- Only with the explicit consent of the customer, Other 'optional' customer details/additional information, if required may be obtained separately after the account is opened.

5.2.2 (I) <u>Customer Due Diligence requirements (CDD) while opening accounts</u>

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 'individuals' and 'Legal Entities' as the case may be. Government of India has authorised the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification dated November 26, 2015.

The 'live run' of the CKYCR would start in phased manner. Accordingly, in the first phase, branches shall upload the KYC data with CERSAI, in respect of new individual accounts opened during the day. Bank shall prepare a plan for uploading the data in respect of existing individual accounts into CKYCR server.

A) <u>Accounts of individuals</u>

1. <u>Accounts of individuals</u>

While establishing an account based relationship or while dealing with the individual who is 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

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

(bb) 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;

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.

d. Branch shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India.

e. Further, if customer wants to provide a current address which is different from the address as per the identity information available in the Central Identities Data Repository, he shall give a self-declaration to the bank.

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

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

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

i. Provided that for a period not beyond such date as may be notified by the Government for a class of banks, 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.

2. 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.

- 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.

- 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.
- For other customers, Branches can use physical copy of the Aadhaar card as well as e-Aadhaar, 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).

It is noted that as per the opinion of the Attorney General, Banks would be entitled to seek authentication of the beneficiaries, who are availing subsidies/ benefits/ services, for the purpose of transfer of any monetary subsidy or benefit to the bank account of the beneficiary, as well as for facilitating the withdrawal of money by the beneficiary through Aadhaar based micro-ATM machines. Accordingly, the Aadhaar enabled Payment System (AePS) and BHIM Aadhaar Pay shall remain operative and bank may continue to maintain and provide these facilities so that the DBT beneficiaries can conveniently withdraw their money through the micro-ATMs, AePS, BHIM Aadhaar Pay etc. without having to visit bank branches which are, in many cases, far away from the places where they live.

From the above there is also no bar on the Banks to perform Aadhaar based authentication using e-KYC authentication facility for opening bank accounts of the client who gives a declaration that s/he is desirous of receiving her/his entitled benefits or subsidies of welfare schemes funded from the Consolidated Fund of India in her/his account directly. Banks may therefore use Aadhaar e-KYC for such clients.

For clients who are not beneficiaries of the aforesaid welfare schemes or who do not give the declaration as mentioned above, as per the Aadhaar judgement and opinion given by Ld Attorney General Banks cannot use Aadhaar E-KYC authentication for opening bank accounts etc. However, they are not prohibited from accepting physical Aadhaar card/E-Aadhaar card/Masked Aadhaar/Offline Electronic Aadhaar xml (if offered voluntarily by the client) for the purpose of opening bank accounts in such cases and verifying the authenticity through QR code etc.

The Attorney General has opined that the voluntary use of a physical Aadhaar card, without authentication, by the Aadhaar number holder who wishes to establish his/her identity, is not prohibited by the judgment. This would include physical copies of 'e-Aadhaar' and 'masked Aadhaar' and offline xml as well. It would also, in my view, permit offline verification of the Aadhaar card, to establish its genuineness through QR code embedded in the Aadhaar card. Accordingly, banks and RBI are at the liberty to use physical copy of the Aadhaar card as well as e-Aadhaar, masked Aadhaar and offline electronic Aadhaar xml provided by UIDAI, which are various forms of Aadhaar, as Officially Valid Documents (OVD) for KYC purpose. However, as per Aadhaar Regulations, the Banks must mask the first 8 digits of the Aadhaar number while storing the physical copy of the Aadhaar card or e-Aadhaar.

For the convenience of such non-DBT beneficiary clients and to avoid paper based manual process, banks are also at liberty and are encouraged to develop a fully electronic web/mobile application which can use the QR code printed on Aadhaar card/ E-Aadhaar/ Masked Aadhaar/ offline Electronic Aadhaar xml (which contain UIDAI's digitally signed KYC information in electronic form), if offered voluntarily, for opening bank accounts. This will make the account opening process completely paperless and hassle-free even for a non-DBT beneficiary client whose bank account, in view of Supreme Court's Judgment, is not permissible to be opened through online Aadhaar authentication.

Since Banks will be using facility of Aadhaar e-KYC for the purpose of opening bank accounts and withdrawal of money through AePS by DBT beneficiaries, it will be mandatory for the banks to provide Aadhaar enrolment facilities. Therefore, every Scheduled Commercial Bank to provide Aadhaar enrolment and update facilities to its customers shall continue to operate.

3. <u>Introduction of accounts</u>

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.

4. <u>Simplified Measures for Proof of Identity</u>

If an individual customer does not have Aadhaar or PAN or any of the OVDs (as mentioned in <u>para 4.9</u> as proof of identity, then 'simplified measures' shall be applied in the case of 'Low risk' customers taking into consideration the type of customer, business relationship, nature and value of transactions based on

the overall money laundering and terrorist financing risks involved. Accordingly, in respect of low risk category of customers, where simplified measures are applied, it would be sufficient to obtain any one of the documents referred under para 2.3.1, which will be deemed as an OVD for the purpose of proof of identity.

5. 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.

6. Simplified Measures for Proof of Address:

The additional documents mentioned under para 4.9 shall be deemed to be OVDs under-simplified measure for the low risk customers for the limited purpose of proof of address where customers are unable to produce any OVD for the same.

7. 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 authorised 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 authorised signatories, photographs of the new signatories are to be obtained duly countersigned by the competent authorities of the concerned institutions/ organisations.

Photograph should be obtained in case of NRI accounts also.

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

8. 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.

9. 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.

- 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.
- 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.

10. 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 "Maha Bank Lok Bachat Yojana" 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:

- accounts where aggregate of all credits in a financial year does not exceed Rs. 1.00 Lakh;
- the aggregate of all withdrawals and transfers in a month does not exceed Rs. 10,000/- and
- Where the balance at any point of time does not exceed Rs. 50,000/- .

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

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 "Maha Bank Lok Bachat Yojana" 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.

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

Officially Valid Documents.
Foreign remittances shall not be allowed to be credited into a The "Maha Bank Lok Bachat Yojana" account unless the identity of the customer is fully established through the production of officially valid documents.

11. Basic Savings Bank Deposit Accounts

The "Basic Savings Bank Deposit Account" is a small account as explained above and shall offer following minimum common facilities to all the customers:

a. The Basic Savings Bank Deposit Account shall be considered a normal banking service available to all.
b. This account shall not have the requirement of any minimum balance.
c. The services available in the account will include deposit and withdrawal of cash at bank branch as well as ATMs; receipt/credit of money through electronic payment channels or by means of deposit/ collection of cheques drawn by Central/ State Government agencies and departments.
d. While there will be no limit on the number of deposits that can be made in a month, account holders will be allowed a maximum of four withdrawals in a month, including ATM withdrawals; and
e. Facility of ATM card or ATM-cum-Debit Card.

The above facilities will be provided without any charges. Further, no charge will be levied for non-operation / activation of inoperative Basic Savings Bank Deposit Account. Additional value added services beyond the stipulated basic minimum services will be chargeable.

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. If such account is opened on the basis of simplified KYC norms, the account would additionally be treated as a "Small Account" and would be subject to conditions stipulated for such accounts as detailed under para 5.2.2 A (10).

Account holders of Basic Savings Bank Deposit Account will not be eligible for opening any other savings bank deposit account in the Bank, if a customer has any other existing savings bank deposit account in the Bank, he/she will be required to close it.

12. A customer is required to submit only one certified Officially Valid Document (OVD) for both proof of identity and for proof of address as part of KYC procedure. If the OVD submitted for proof of identity does not have the proof of address (for e.g., PAN Card), then the customer is required to submit another OVD for proof of address.

13. Similarly, a customer is required to submit only one certified OVD as proof of address (either current or permanent) for KYC purpose. In case the proof of address furnished by the customer is neither the local address nor the address where the customer is currently residing, the branch shall take a declaration of the local address on which all correspondence will be made by the Bank with the customer.

No address proof is required to be submitted for such address for correspondence / local address. This address shall be verified by the branch through 'positive confirmation' such as acknowledgment of receipt of

- letter, cheque books, ATM cards;
- telephonic conversation;
- Visits; etc.

In the event of change in this address due to relocation or any other reason, customers may intimate the new address for correspondence to the Bank within two weeks of such a change.

14. In case the address mentioned as per 'proof of address' undergoes a change, fresh proof of address should be submitted to the branch within a period of six months.

15. In case of close relatives, such as husband, wife, son, daughter and parents etc. who live with their wife, husband, father/ mother, daughter and son, who do not have Officially Valid Document for address verification, then, in such cases, Branches shall obtain an OVD for proof of address and identity of the relative with whom the prospective customer is living, together with a declaration from the relative that the said person (prospective customer) proposing to open an account is a relative and is staying with relative.

16. Branches are not required to obtain fresh documents of customers when customers approach them for transferring their account from one branch of the Bank to another branch. KYC once done by one branch of the Bank shall be valid for transfer of the account within the Bank if full KYC verification has been done for the concerned account and is not due for periodic updation explained in **5.2.2 (III)**. The customer shall be allowed to transfer his account from one branch to another branch without restrictions.

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

If an existing KYC compliant customer of the Bank desires to open another account in the Bank, there should be no need for submission of fresh proof of identity and/or proof of address for the purpose.

17. Where a customer categorised as low risk expresses inability to complete the documentation requirements on account of any reason that the bank/branch considers to be genuine, and where it is essential not to interrupt the normal conduct of business, the branch may complete the verification of identity within a period of six months from the date of establishment of the relationship.

18. 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 conditions that-

- The branch immediately obtains necessary information of such client due diligence carried out by the third party;
- 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;
- The branch is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record- keeping requirements in line with the requirements and obligations under the PML Act;
- The third party is not based in a country or jurisdiction assessed as high risk; and
- The branch is ultimately responsible for customer due diligence and undertaking enhanced due diligence measures, as applicable.

19. <u>Accounts of non-face-to-face customers</u>

With the introduction of phone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. In the case of non-face-to-face customers (i.e., customers who open accounts without visiting the branch/offices of the Bank or meeting the officials of the Bank), apart from applying the usual customer identification procedures, there shall be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented shall be insisted upon and, if necessary, additional documents shall ask to submit. In such cases, Bank may also require the first payment to be effected through the customer's account with another bank which, in turn, follows KYC procedures.

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

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, bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other bank shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

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.

20. <u>Accounts opened using OTP based e-KYC</u>

Accounts opened 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. The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete.
iii. The aggregate of all credits in a financial year, in all the deposit accounts taken together, shall not exceed rupees two lakh.
iv. As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.
v. Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which identification is to be carried out.
vi. If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.
vii. A declaration is to 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, 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.

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

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.

22. Introduction of Video based Customer Identification Process (V-CIP)

On January 10, 2020 the Reserve Bank of India (**RBI**) has introduced Aadhaar-based **Video Customer Identification Process (V-CIP**). This process will allow banks to complete the KYC (Know Your Customer) process of customers on video itself. This facility can be used as an alternative to the already available e-KYC facility. To introduce V-CIP, RBI has amended guidelines under the Prevention of Money-laundering (Maintenance of Records) Rules, **2005**.

Reserve Bank of India (RBI) has now allowed video-based know-your-customer (KYC) identification process that will provide an additional method of customer on-boarding. The video-based know-your-customer (KYC) identification process is carried out by a branch official of the bank for establishing account based relationship with an individual customer. Video-based know-your-customer (KYC) identification process is the alternate method of establishing the customer's identity.

But this new facility also puts a lot of responsibility on the banks, which requires use of latest technological tools, ensuring live location and interaction, training of people, storage etc.

The branch official of the bank record video as well as capture photograph of the customer present for identification and obtain the identification information. The identification information is as follows:

- OTP based Aadhaar e-KYC authentication or Offline Verification of Aadhaar for identification.
- Services of Business Correspondents (BCs) may be used by banks for aiding the V-CIP

KYC application can be accessed only through login-id and password or Live OTP or Time OTP.

Use of latest technology and tools

Banks will have to use the latest technologies in the market like artificial intelligence, face matching tools etc to ensure the integrity of the video KYC process as well as the information furnished by the customer. The entire responsibility of customer identification lies with the bank as they have to ensure that the person who is live is the same person who has provided his other identification details. They would have to ensure the same by matching the picture with the person and also validating the location.

As per the RBI directives, the reporting entity should 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. Adding to it, the photograph of the customer in the Aadhaar/PAN details should be verified from the database of the issuing authority.

Capturing live location

The bank has to capture and ensure that the customer is physically present in India and not outside India. This can be done by geotagging, which helps in locating the exact place and time the picture or video was taken. The audio visual interaction will be triggered from the domain of the bank only and not from any third party service provider.

Ensuring real interaction

The bank official will also have to ensure that the sequence and the type of questions asked during the video interactions are varied to establish that the interactions are real-time and not pre-recorded. They will also have to ensure that the process is seamless, in real-time, secured and is end-to-end encrypted.

The banks will also have to carry out liveliness check in order to guard against spoofing and other fraudulent manipulations.
The RBI makes it clear that all accounts opened through video KYC will be operational only after ensuring the integrity of the new process. In fact, the banks have to test the system for security, robustness and end-to-end encryption. They will have to carry out software and security audit and validation of the video KYC application before rolling it out.

Storage and training of people

The bank will have to ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp. In fact, the entire process will be handled by officials specifically trained for this purpose. The activity, along with credentials of the officials performing the video process will be preserved for future records.

Here are the steps for video-based KYC:

1) The bank will initially develop an application for the digital KYC process that will be made available at customer touch points for undertaking KYC of their customers.
2) The application will be accessed only through login-id and password or Live OTP or Time OTP. The customer, for the purpose of KYC, will have to visit the location of the authorised official of the bank or vice-versa.
3) The background behind the customer while capturing live photograph should be of white colour and no other person should come into the frame while capturing the live photograph of the customer. The live photograph of the officially valid document should be captured vertically.
4) All the entries in the application form will be filled according to the documents and information furnished by the customer.
5) In the documents where Quick Response (QR) code is available, such details will be auto-populated by scanning the QR code instead of manual filing of details.
6) 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' would be sent to customer's mobile number.
7) Upon successful validation of the OTP, it will be treated as customer signature on the application.
8) The application will then give message about the completion of the process. The authorised officer will further check and verify if the live photograph of the customer matches with the photo available in the document and all other necessary details.
9) On successful verification, the application form should be digitally signed by authorised officer.
10) He will then take a print of the application form, 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, RBI mentioned in the circular.

23. 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:-

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.

- 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.
- During the 30 days period, the account should be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of monthly withdrawal to Rs. 50,000/-, pending verification of address.
- 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.
- Students with Pakistani nationality will need prior approval of the Reserve Bank of India for opening the account.

24. <u>Accounts of Politically Exposed Persons (PEPs) resident outside India</u>

Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/ Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Bank is to 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 should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. Bank should subject such accounts to enhanced monitoring on an ongoing basis. Branches shall maintain a database of PEP accounts in the Branch. The above norms should also be applied to the accounts of the family members or close relatives of PEPs.

In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, 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 should 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 should 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.

B) Accounts of persons 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.

RBI vide its notifications dated 15.05.2004 and 02.07.2015 has instructed all Banks that at the time of opening of Current Accounts, Bank shall insist on declaration from the account holder to the effect that he is not enjoying any credit facility with any other bank or obtain a declaration giving particulars of credit facilities enjoyed by the intending customer with any other bank(s).

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.

1. Accounts of Proprietary Concerns

For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.

For Proprietary concerns, in addition to the Officially Valid Documents applicable to the individual (proprietor), any two of the following documents or the equivalent e- documents there of as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

- Registration Certificate
- Certificate / license issued by the Municipal authorities under Shop & Establishment Act.
- Sales and income tax returns.
- CST/VAT/ GST certificate (provisional/final).
- Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities.
- IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
- Licence / certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
- complete Income Tax return (not just the acknowledgement) in the name of the sole Proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax Authorities.

- 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.

2. Accounts of Companies

Where the client is a company, certified copies of all the following documents or the equivalent e-documents are to be submitted:

- Certificate of incorporation
- Memorandum and Articles of Association
- Permanent Account Number of the Company
- A resolution from the Board of Directors and Power of Attorney granted to its managers, officers or employees to transact on its behalf.
- Documents as specified in 5.2.2 A (1), relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.

3. Accounts of Partnership firms

Where the client is a partnership firm, certified copies of all the following documents or the equivalent e-documents are to be submitted:

- Registration Certificate
- Partnership Deed
- Permanent Account Number of the Partnership Firm
- Documents as specified in 5.2.2 A (1), relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf

4. Accounts of Trusts

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

- Registration Certificate
- Trust Deed
- Permanent Account Number or Form 60/61 of the Trust
- Documents as specified in 5.2.2 A (1), relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.

5. Accounts of Unincorporated association or a body of individuals

a) 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 are to be submitted:

- Resolution of the managing body of such association or body of individuals
- Permanent Account Number or Form 60/61 of the Unincorporated association
- Power of Attorney granted to the person who will transact on its behalf.
- Documents as specified in 5.2.2 A (1), relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf and
- Such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals.

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

b) For opening accounts of **juridical persons such as Governments or its Departments, Societies, Universities and Local Bodies like Village Panchayats**, certified copies of all the following documents shall be obtained:
   - Document showing name of the person authorized to act on behalf of the entity;
   - Documents as specified in 5.2.2 A (1), of the person holding an attorney to transact on its behalf and
   - Such documents as may be required by the Bank to establish the legal existence of such an entity/ juridical person.

6. Accounts of Foreign Portfolio Investors (FPIs) for Portfolio Investment Scheme (PIS)

In terms of Rule 9 (14)(i) of the PML Rules, 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. 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.

For this purpose, branches may rely on the KYC verification done by the third party (i.e. the Custodian/SEBI Regulated Intermediary) subject to the conditions laid down in Rule 9 (2) [(a) to (e)] of the PML Rules.

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

authorised representative. While transferring such documents, the Custodian/Regulated Intermediary shall certify that the documents have been duly verified with the original or notarised 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.

7. Client accounts opened by professional intermediaries

When the Bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client 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 client confidentiality that prohibits disclosure of the client details to the Bank. Where funds held by the intermediaries are not co-mingled at the Bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners 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.

8. Opening of Current Account with non-consortium banks

In terms of extant guidelines of lending under consortium, a bank which is not a member of a consortium/syndicate, shall not open current account or extend any banking facility without the concurrence of the consortium/syndicate. This shall be scrupulously complied with.

9. 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:

a. KYC verification of all the members of SHGs need not be done while opening the Savings Bank account of the SHGs and KYC verification of all the office bearers would suffice.
b. As regards KYC verification at the time of credit linking of SHGs, no separate KYC verification of the members or office bearers is necessary.

10. Identification of Beneficial Ownership

Rule 9(3) of the Prevention of Money Laundering Rules, 2005 requires that every banking company, and financial institution, as the case may be, shall identify the beneficial owner and take all reasonable steps to verify his identity. The term "Beneficial Owner" has been defined as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person.

A juridical person is an Entity that is not a single natural person (as a human being), authorized by law with duties and rights, recognized as a legal authority having a distinct identity, a legal personality (Also known as artificial person, juridical entity, juristic person, or legal person).

The procedure for determination of Beneficial Ownership as per RBI/Government guidelines is as under:

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

Explanation - For the purpose of this sub-clause-

- "Controlling ownership interest" means ownership of or entitlement to more than twenty-five percent of shares or capital or profits of the company;
- "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

b. where the client is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of/entitlement to more than fifteen percent of capital or profits of the partnership;
c. where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;

d. where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;
e. where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and
f. Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

There exists the possibility that trust / nominee or fiduciary accounts can be used to circumvent the customer identification procedures. In such cases, Bank shall determine whether the customer is acting on behalf of another person as trustee / nominee or any other intermediary. If so, Bank shall insist on satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. The different categories of beneficiaries should be identified as defined above. In the case of a 'foundation', steps shall be taken to verify the founder managers / directors and the beneficiaries, if defined.

11. Accounts of Non Profit Organisations

A 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 Section 8 of the Companies Act 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 lac, the Bank shall consider filing a Suspicious Transaction Report to FIU-IND.

12. 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.

5.2.2 (II) 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 favour anonymity, and take measures, if needed, to prevent the same being used for money laundering 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.

Bank shall ensure that appropriate KYC procedures are duly applied before issuing

the cards to the customers. Bank 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 KYC measures.

5.2.2 (III) Periodic Updation of KYC

A) CDD requirements for periodic updation

Bank shall have a system of periodical updation of customer identification data (including photograph/s) as under:

i. Branches should apply client due diligence measures/full KYC exercise to existing clients at least every two years for High Risk customers, every eight years for Medium Risk customers and every ten years for Low Risk customers taking into account whether and when customer due diligence measures have previously been undertaken and the adequacy of data obtained.

Full KYC exercise may include all measures for confirming identity and address and other particulars of the customer that the Bank may consider reasonable and necessary based on the risk profile of the customer. The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

Branches shall ensure that KYC documents, as per extant requirements of the Master Direction, are available with them.

Branches should carry out **ongoing due diligence** of existing clients in order to ensure that their transactions are consistent with the Bank's knowledge of the client, his business and risk profile and where necessary, the source of funds.

Branches should undertake client due diligence (CDD) measures while commencing an account-based relationship. Such measures include identifying and verifying the customer and beneficial owner on the basis of reliable and independent information and data or documents.

The periodical verification / updation of customer data shall be done irrespective of whether the account has been transferred from one branch to another and Bank shall maintain records of transactions as prescribed.

Apart from home branches, the branches other than Home Branch also shall perform Full KYC exercise / Positive confirmation, whenever the customer approaches that branch and requests the branch to complete the Full KYC exercise / Positive confirmation by submitting the required documents. Such branches should exercise due diligence in verification of the documents and updation of the details in the CBS system.

ii. Branches need not seek fresh proofs of identity and address at the time of periodic updation from those customers who are categorised as 'low risk', in case of no change in status with respect to their identities and addresses. A self-certification by the customer to that effect should suffice in such cases. In case of change of address of such 'low risk' customers, they could merely forward a certified copy of the document (proof of address) by mail/post, etc. Branches need not insist on physical presence

of such low risk customer at the time of periodic updation.

iii. Fresh photographs and Officially Valid Documents shall be obtained from minor customer on becoming major.

iv. 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 client an accessible notice and a reasonable opportunity to be heard. Further, RE shall include, in its internal policy, 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.

B) <u>Freezing and Closure of accounts</u>

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.

5.2.2 (IV) <u>Miscellaneous</u>

A) <u>Period for presenting payment instruments</u>

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) <u>Collection of Account Payee Cheques</u>

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 co-operative credit societies.

C) <u>At par cheques facility availed by co-operative banks</u>

Some commercial banks have arrangements with co-operative banks under which the latter open current accounts with the commercial banks and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in-customers for effecting their remittances and payments. Since the 'at par' cheque facility offered by commercial banks to co-operative banks is in the nature of correspondent banking arrangements, branches maintaining/opening such accounts should monitor and review such arrangements to assess the risks

including credit risk and reputational risk arising therefrom. For this purpose, branches should retain the right to verify the records maintained by the client cooperative banks / societies for compliance with the extant instructions on KYC and AML under such arrangements.

D) Operation of Bank Accounts & Money Mules

Money Mules are individuals with bank accounts who are recruited by fraudsters to receive cheque deposit 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 minimize the operations of such mule accounts, Branches should strictly adhere to the guidelines on opening of accounts and monitoring of transactions.

E) 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.

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

Any remittance of funds by way of Demand Draft 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.

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 15th September 2018.

G) Sale of third party products

When Bank sells third party products as 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:

a. Even while selling third party products as agents, branches should verify the identity and address of the walk-in customer.
b. 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 paragraph 8 below (Maintenance of KYC documents and preservation

period).

c. 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.
d. Sale of third party products by branches as agents to customers, including walk-in customers, for Rs. 50,000/- and above must be
    - by debit to customer's account or against cheques and
    - obtention & verification of the PAN given by the account based as well as walk-in customers.

This instruction would also apply to sale of bank's own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for Rs. 50,000/- and above.

H) <u>Prohibition on dealing in Virtual Currencies (VCs).</u>

Entities regulated by the RBI shall not deal in VCs or provide services for facilitating any person or entity in dealing with or settling VCs with immediate effect.

5.3 <u>Monitoring of Transactions</u>

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:

- The extent of monitoring will depend on the risk category of the account. High risk accounts have to be subjected to more intensify monitoring.
- Branches should pay particular attention to the following types of transactions:
    a. Large and complex transactions, and those with unusual patterns, which have no apparent economic rationale or legitimate purpose.
    b. Transactions which exceed the thresholds prescribed for specific categories of accounts.
    c. Transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer.
    d. High account turnover inconsistent with the size of the balance maintained.
- 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 categorisation of customers shall be carried out at a periodicity of not less than once in six months.
- Branches closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies. Branches should analyse 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.

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

5.4 Risk Management

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.

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".

Operational Risk 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."

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".

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.

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 client 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:

- Using a risk-based approach to address management and mitigation of various AML/CFT risks.
- Allocation of responsibility for effective implementation of policies and procedures.
- Independent evaluation by the compliance functions of Bank's policies and procedures, including legal and regulatory requirements.
- Concurrent/internal audit/snap audit to verify the compliance with KYC/AML policies and procedures.
- Putting up consolidated note on such audits and compliance to the Audit Committee at quarterly intervals and to Board of Directors at monthly intervals by AML Department, 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:

- 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.

- Customers who are likely to pose a higher than average risk shall be categorised 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.

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 client and obtaining information on the purpose and intended nature of business relationship.

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

The roles and responsibilities of various Departments with regard to KYC/AML/CFT matters are as follows:

Planning Department-

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

TIBD-

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

AML Cell, Inspection & Audit Department, RBS & MIS Department-

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

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:

a) 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.

b) 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.
c) The responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented.
d) In the case of payable-through-accounts, 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.
e) Bank shall also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.
f) 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.
g) 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.
h) 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).
i) Bank shall not permit its accounts to be used by shell banks.

7. WIRE TRANSFERS

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

(1) The salient features of a wire transfer transaction are as under:

- Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. The originator and the beneficiary may be the same person.
- Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institutions are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.
- Domestic wire transfer means any wire transfer where the originator

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

- The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the bank to perform the wire transfer.

(2) Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and / or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analysing suspicious or unusual activity and disseminating it as necessary.

The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits.

Accordingly, Bank shall ensure that all wire transfers are accompanied by the following information.

7.1 Cross-border wire transfers

- All cross-border wire transfers must be accompanied by accurate and meaningful originator information.
- Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included.
- Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (2) above.

7.2 Domestic wire transfers

- Information accompanying all domestic wire transfers of Rs. 50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.
- If the Bank has reason to believe that a customer is intentionally structuring wire transfers to below Rs. 50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the Bank shall insist on complete customer identification

before effecting the transfer. In case of non-cooperation from the customer, efforts shall be made to establish his identity and Suspicious Transaction Report (STR) shall be made to FIU-IND.

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

(3) **Exemptions**

Inter-bank transfers and settlements where both the originator and beneficiary are banks or financial institutions would be exempted from the above requirements.

(4) **Role of Ordering, Intermediary and Beneficiary Banks**

(a) Ordering Bank

An Ordering Bank is the one that originates a wire transfer as per the order placed by its customer. As Ordering Bank, the Bank shall ensure that qualifying wire transfers contain complete originator information. The Bank shall also verify and preserve the information at least for a period of five years.

(b) Intermediary Bank

For both cross-border and domestic wire transfers, Bank processing an intermediary element of a chain of wire transfers shall ensure that all originator information accompanying a wire transfer is retained with the transfer. Where technical limitations prevent full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record shall be kept at least for five years (as required under Prevention of Money Laundering Act, 2002) as the receiving Intermediary Bank, of all the information received from the Ordering Bank.

(c) Beneficiary Bank

A Beneficiary Bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they should be reported to the Financial Intelligence Unit-India. As Beneficiary Bank, the Bank shall also take up the matter with the Ordering Bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information on the remitter, the Bank shall consider restricting or even terminating its business relationship with the Ordering Bank.

8. MAINTENANCE OF KYC DOCUMENTS AND PRESERVATION 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 have a system of maintaining proper record of transactions

prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005), as mentioned below:

A. All cash transactions of the value of more than Rupees ten lakh or its equivalent in foreign currency;

B. Series of all cash transactions integrally connected to each other which have been individually valued below Rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of Rupees ten lakh or its equivalent in foreign currency;

BA. All transactions involving receipts by non-profit organisations of value more than Rupees ten lakh, or its equivalent in foreign currency;

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

D. All suspicious transactions whether or not made in cash and by way of-

   i. Deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of –
      a. Cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or
      b. Travellers cheques, or
      c. Transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts, or
      d. Any other mode in whatsoever name it is referred to;
   ii. Credits or debits into or from any non-monetary accounts such as D-mat account, security account in any currency maintained by the banking company, financial institution and intermediary, as the case may be;
   iii. Money transfer or remittances in favour of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by any of the following:
      a. Payment orders, or
      b. Cashiers cheques, or
      c. Demand drafts, or
      d. Telegraphic or wire transfers or electronic remittances or transfers, or
      e. Internet transfers, or
      f. Automated Clearing House remittances, or
      g. Lock box driven transfers or remittances, or

h. Remittances for credit or loading to electronic cards, or
i. Any other mode of money transfer by whatsoever name it is called;

iv. Loans and advances including credit or loan substitutes, investments and contingent liability by way of-
   a. subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitised participation, inter-bank participation or any other investments in securities or the like in whatever form and name it is referred to, or
   b. purchase and negotiation of bills, cheques and other instruments, or
   c. foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called, or
   d. Letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/or credit support;

v. Collection services in any currency by way of collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to.

E. 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;

F. All purchase and sale by any person, of immovable property valued at Rupees fifty lakh or more that is registered by the reporting entity, as the case may be.

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:

a. The nature of the transactions;
b. The amount of the transaction and the currency in which it was denominated;
c. The date on which the transaction was conducted; and
d. The parties to the transaction.

8.2 <u>Preservation of Records</u>

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.

i. 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.

ii. Bank shall ensure that records pertaining to the identification of the customers and their address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended as required under Rule 10 of the Rules ibid. 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. 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):

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/resou rces/xsl/en/al-qaida-r.xsl*

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/resou rces/xsl/en/tal i ban-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 customer ID/opening of accounts. Branches are required to ensure that the names/s of the proposed customer does not

match with that of the UN list of Terrorist individuals/organization/ entities, before opening any new account. Branches are also required to cross check the details of all existing accounts with the updated list 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, branches have to verify transactions carried out in such accounts and report those accounts to RBI/Financial Intelligence Unit-INDIA, New Delhi.

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

A. 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.

B. Bank shall strictly follow the procedure laid down in the UAPA Order dated March 14, 2019 (Annexure II of this policy) and ensure meticulous compliance with the Order issued by the Government.

9.2 Jurisdictions that do not or insufficiently apply the FATF Recommendations

Bank shall take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the Financial Action Task Force (FATF) Statement. In addition to FATF Statements circulated by Reserve Bank of India from time to time, Bank shall also consider publicly available information for identifying countries, which do not or CKYCinsufficiently apply the FATF Recommendations. Bank shall also give special attention 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.

Bank shall examine 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. Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions shall, as far as possible be examined, and written findings together with all documents shall be retained and made available to Reserve Bank/other relevant authorities, on request.

10. REPORTING REQUIREMENTS

10.1 Reporting to Financial Intelligence Unit-India

i. 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 nonprofit 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, Hotel Samrat, Chanakyapuri, New Delhi-110021. Website - http://fiuindia.gov.in/

ii. 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 FINnet dated 31st March, 2011 by FIU containing all relevant details are available on FIU's website.

iii. 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:

- The Bank shall communicate to the Director, FIU-IND the name, designation and address of the Designated Director and the Principal Officer.
- The Principal Officer shall furnish the information referred to in clauses (A), (B), (BA), (C), (D), (E), (F) to the Director on the basis of information available with the reporting entity (details of above clauses are furnished under para 10.1). A copy of such information shall be retained by the Principal Officer for the purposes of official record.
- The Bank shall evolve an internal mechanism having regard to any guidelines issued by regulator, for detecting the transactions referred to in clauses (A), (B), (BA), (C), (D), (E) and (F) for furnishing

information about such transactions in such form as may be directed by its Regulator.

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

10.2 Reports to be furnished to FIU-IND

10.2.1 Cash Transaction Reports (CTR)

The Bank shall scrupulously adhere to the following:

i. 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 FIU-IND within the prescribed time schedule.

ii. 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.

iii. While filing CTR, details of individual transactions below Rupees Fifty Thousand need not be furnished.

iv. 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.

v. 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 FIUIND. 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 centralised 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.

vi. 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.

vii. The instruction on 'Maintenance of records of transactions' and 'Preservation of records' as contained at Para 6 (i) and (ii) respectively shall be scrupulously followed by the branches.

10.2.2 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 involve 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.

10.2.3 Non-Profit Organisations (NPO)

The report of all transactions involving receipts by non-profit organisations 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.

10.2.4 Cross-border Wire Transfer Report

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 FIU-IND.

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 Sensitising Customers

Implementation of AML/CFT policy may require certain information from customers of a personal nature or which had not been called for earlier. The purpose of collecting such information could be questioned by the customer and may often lead to avoidable complaints and litigation. 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.

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.

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.

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

In terms of the Foreign Contribution Regulation Act, 2010, certain categories of individuals and organizations are required to obtain prior permission from the Central Government (Secretary, Ministry of Home Affairs, GOI, New Delhi) to receive "Foreign Contributions" or accept "Foreign Hospitality" and such receipts/acceptance require reporting to the Government.

- **Individuals / Organisations who cannot receive foreign contributions :** Foreign contributions cannot be accepted by candidate for election, correspondent, columnist, cartoonist, editor, owner, printer or publisher of a registered newspaper, judge, Government servant or employee of any corporation, member of any legislature, political party or office bearer thereof.
- **Individuals/Organisations who can receive foreign contributions:** An association having a definite cultural, economic, educational, religious or social programme can receive foreign contribution after it obtains the prior permission of the Central Government or gets itself registered with the Central Government.

Bank shall ensure that the provisions of the Foreign Contribution (Regulation) Act, 2010, wherever applicable, are strictly adhered to.

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.

****

ANNEXURE – I
Digital KYC Process

1. The RE 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 REs.
2. The access of the Application shall be controlled by the REs 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 REs to its authorized officials. C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the RE or vice-versa. The original OVD shall be in possession of the customer.
3. The RE 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 watermark in readable form having CAF number, GPS coordinates, authorized official's name,

unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

4. The Application of the RE 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.
5. 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.
6. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
7. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.
8. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the RE shall not be used for customer signature. The RE must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.
9. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the RE. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.
10. 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 RE, 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.
11. The authorized officer of the RE shall check and verify that:- (i) information vailable 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;

12. On Successful verification, the CAF shall be digitally signed by authorized officer of the RE who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer. Banks may use the services of Business Correspondent (BC) for this process.

ANNEXURE – II

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

1. In respect of funds, financial assets or economic resources or related services held in the form of bank accounts, the RBI would forward the designated lists to the banks. The RBI would issue necessary guidelines to banks, requiring them to:-

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

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

iii) The banks shall also send by post a copy of the communication mentioned in (ii) above to the UAPA nodal officer of the state/ UT where the account is held and Regulators and FIU-IND, as the case may be.

iv) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt**,** the banks would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (CTCR), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail jsctcr-mha@gov.in.

v) The banks shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (ii) above, carried through or attempted, as per the prescribed format.

2. On receipt of the particulars referred to in para a (ii) above, CTCR Division of MHA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/entities identified by the banks are the ones listed as designated individuals / entities and the funds, financial assets or economic resources or related services, reported by banks are held by the designated individuals/entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

3. In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned bank branch under intimation to respective Regulators and FIU-IND. The UAPA nodal officer of CTCR Division of MHA shall also forward a copy thereof to all the Principal Secretary/Secretary, Home Department of the States or UTs, so that any individual or entity may be prohibited from making any funds, financial assets or economic 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 UAPA nodal officer of CTCR Division of MHA shall also forward a copy of the order under Section 51A, to all Directors General of Police/Commissioners of Police of all states/UTs for initiating action under the provisions of Unlawful Activities (Prevention) Act. The order shall take place without prior notice to the designated individuals/entities.

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

4. CTCR Division of MHA would electronically forward the designated lists to the UAPA nodal officer of all States/UTs with the 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.

5. 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 Joint Secretary (CTCR), Ministry of Home Affairs, immediately within 24 hours at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail jsctcr-mha@gov.in.

6. 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 would be completed within a maximum of 5 working days and should be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual/entity to Joint Secretary (CTCR), Ministry of Home Affairs at the Fax telephone numbers and also on the e-mail.

7. A copy of this reference should be sent to the Joint Secretary (CTCR), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail**.** MHA may have the verification also conducted by the Central Agencies. This verification would be completed within a maximum of 5 working days.

8. In case, the results of the verification indicate that the particulars match with those of designated individuals/entities, an order under Section 51A of the UAPA would be issued within 24 hours, by the nodal officer of CTCR Division of MHA 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 take place without prior notice, to the designated individuals/entities.

9. 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 coming to his notice, transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State/UT for also initiating action under the provisions of Unlawful Activities (Prevention) Act.

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

10. U.N. Security Council Resolution 1373 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.

11. To give effect to the requests of foreign countries under 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 UAPA nodal officer for CTCR Division for freezing of funds or other assets.

12. The UAPA nodal officer of CTCR Division of MHA, shall cause the request to be examined, within 5 working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request 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.

13. Upon receipt of the requests by these nodal officers from the UAPA nodal officer of CTCR Division, the procedure as enumerated at paragraphs 1 to 9 above shall be followed. The freezing orders shall take place without prior notice to the designated persons involved.

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

14. 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.

15. 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.

16. The Joint Secretary (CTCR), MHA, being the nodal officer for (CTCR) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within 15 working days, 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 and the nodal officers of States/UTs. However, if it is not

possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of CTCR Division shall inform the applicant.

Communication of Orders under section 51A of Unlawful Activities (Prevention) Act.

17. All Orders under section 51A of Unlawful Activities (Prevention) Act, relating to funds, financial assets or economic resources or related services, would be communicated to all banks through respective Regulators, and to all the Registrars performing the work of registering immovable properties, through the State/UT nodal officer by CTCR Division of MHA.

Regarding prevention of entry into or transit through India

18. 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.

19. 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.

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

20. The nodal officers of CTCR Division and 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.

ANNEXURE – III

INDICATIVE LIST OF CUSTOMER BEHAVIOUR & RISK BASED TRANSACTION MONITORING

1. 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 Institution to verify.
2. Customer expressing unusual curiosity about secrecy of information involved in the transaction.
3. Customers who decline to provide information that in normal circumstances would make the customer eligible for banking services.
4. Customer giving confusing details about a transaction.
5. 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.
6. Customers who use separate tellers to conduct cash transaction or foreign exchange transactions
7. Customers who deposit cash / withdrawals by means of numerous deposit slips/ cheques leaves so that the total of each deposits is unremarkable, but the total of all credits / debits is significant.
8. Customer's representatives avoiding contact with the branch.
9. Customers who repay the problem loans unexpectedly.
10. Customers who appear to have accounts with several institutions within the same locality without any apparent logical reason.
11. Customers 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.
12. Customer regularly issues large value cheques without balance and then deposits cash.
13. 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

1. Exchanging an unusually large amount of small denomination notes for those of higher denomination;
2. Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;
3. Frequent withdrawal of large amounts by means of cheques, including traveler's cheques;
4. Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;
5. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;
6. Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally

associated with the normal commercial operations of the company, e.g. cheques, letters of credit, bills of exchange etc.;

7. 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

1. A customer having a large number of accounts with the same bank, with frequent transfers between different accounts;
2. Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.

C. Activities not consistent with the Customer's Business

1. Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.
2. Corporate accounts where deposits & 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.
3. Unusual applications for DD/TT/PO against cash.
4. Accounts with large volume of credits through DD/TT/PO whereas the nature of business does not justify such credits.
5. Retail deposit of many cheques but rare withdrawals for daily operations.

D. Attempts to avoid Reporting/Record-keeping Requirements

1. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
2. Any individual or group that coerces/induces or attempts to coerce/induce a bank employee not to file any reports or any other forms.
3. An account where there are several cash deposits/withdrawals below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

E. Unusual Activities

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

F. Customer who provides Insufficient or Suspicious Information

1. A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors, or its locations.
2. A customer/company who is reluctant to reveal details about its activities or to provide financial statements.

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

G. Certain Suspicious Funds Transfer Activities

1. Sending or receiving frequent or large volumes of remittances to/from countries outside India.
2. Receiving large TT/DD remittances from various centers and remitting the consolidated amount to a different account/center on the same day leaving minimum balance in the account.
3. Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire/funds transfer.

H. Certain Bank Employees arousing Suspicion

1. An employee whose lavish lifestyle cannot be supported by his or her salary.
2. Negligence of employees/willful blindness is reported repeatedly.

I. 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.

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

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

Check list for preventing money-laundering activities

1. 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).
2. A customer regularly depositing or withdrawing large amounts by a wire transfer to, from, or through countries that are known sources of narcotics or where Bank secrecy laws facilitate laundering money.
3. A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer's business or history.

4. A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.
5. A customer experiences increased wire activity when previously there has been no regular wire activity.
6. Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.
7. 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.
8. Deposits of currency or monetary instruments into the account of a domestic trade or business, which in turn are quickly wire transferred abroad or moved among other accounts for no particular business purpose.
9. Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.
10. Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.
11. Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency
12. Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.
13. Periodic wire transfers from a person's account/s to Bank haven countries.
14. A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.
15. A customer or a non-customer receives incoming or makes outgoing wire transfers involving currency amounts just below a specified threshold, or that involve numerous Bank or travelers cheques.
16. A customer or a non-customer receives incoming wire transfers from the Bank to 'Pay upon proper identification' or to convert the funds to bankers' cheques and mail them to the customer or non-customer, when
17. The amount is very large (say over Rs. 10 Lakh)
    - The amount is just under a specified threshold.
    - The funds come from a foreign country or
    - Such transactions occur repeatedly.
18. 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)
19. A Non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit.

ANNEXURE – IV
Monitoring of Customer Risk Categorisation (CRC)

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

1. 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.
2. Customer expressing unusual curiosity about secrecy of information involved in the transaction.
3. Customers who decline to provide information that in normal circumstance would make the customers eligible for banking services.
4. Customer giving confusing details about a transaction.
5. 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.
6. Customers who use separate tellers to conduct cash transactions or foreign exchange transactions.
7. Customers who deposit cash/ withdrawals by means of numerous deposit slips/ cheques leaves so that the total of each deposits is unremarkable, but the total of all credits/ debits is significant.
8. Customer's representatives avoiding contact with the branch.
9. Customer who repays the problem loans unexpectedly.
10. Customers who appear to have accounts with several banks within the same locality without any apparent logical reason.
11. 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.
12. Customers regularly issue large value cheques without balance and then deposits cash.
13. Sudden transfer of funds from unrelated accounts through internet (or such other electronic channels) and subsequent quick withdrawal through ATM.

Transactions involving large amounts of cash

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

an account which has just received an unexpected large credit from abroad.

6. Company transactions, both deposits and withdrawals that are denominated by unusually large amounts of cash rather than by way of debits and credits normally associated with the normal commercial operations of the company e.g. cheques , letters of credit , bills of exchange etc.
7. Depositing cash by means of numerous credit slips by a customer, such that the amount of each deposit is not substantial, but the total of which is substantial.

Transactions that do not make Economic Sense

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

Activities not consistent with the customer's business

1. Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.
2. Corporate accounts where deposits and withdrawals by cheque / telegraphic transfers/ foreign inward remittances/ any other means are received from / made to sources apparently unconnected with the corporate business activity/ dealings.
3. Unusual applications for DD/ PO/NEFT/RTGS against cash.
4. Accounts with large volume of credits through DD/ PO/NEFT/RTGS whereas the nature of business does not justify such credits.
5. Retail deposit of many cheques but rare withdrawals for daily operations.

Attempts to avoid reporting/ record- keep requirements

1. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
2. Any individual or group that coerces/ induces or attempts to coerce/ induce a bank employee not to file any reports or any other forms.
3. An account where there are several cash deposits /withdrawals below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customers intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

Unusual Activities

1. An account of a customer who does not reside / have office near the branch even though there are bank branches near his residence/ office.
2. A customer who often visits the safe deposit area immediately before

making cash deposits, especially deposits just under the threshold level.

3. Funds coming from the list of countries / centres, which are known for money laundering.

Customer who provides insufficient or suspicious information

1. A customer / company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors or its locations.
2. A customer / company who is reluctant to reveal details about his/its activities or to provide financial statements.
3. A customer who has no record of past or present employment but makes frequent large transactions.

Certain suspicious funds transfer activities

1. Sending or receiving frequent or large volumes of remittances to/from countries outside India.
2. 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.
3. Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire / fund transfer.

ANNEXURE – V

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	- 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 organisations. - 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

	companies - Blind - Purdanashin - Registered Body - Corporate Body - Joint Sector - Partnership	close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner; - 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 - Client 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 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 Multi-level 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 jewelers (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 - M i n o r - Accounts under Foreign Contribution Regulation Act

The above categorization of customers under risk perception is only illustrative and not exhaustive.

1.	Updating KYC of low risk customers:	Every 10 years.
2.	Updating KYC of medium risk customers:	Every 8 years
3.	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 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

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).

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

ANNEXURE – VI

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	Where the client is an individual, he shall submit:- a. Any Certified copy which contains proof of Identity/ address b. The Permanent Account Number (PAN) or Form 60/61 as defined in the Income Tax Rules, 1962, And such other documents including in respect of the nature of business and financial status of the client as may be required by the Bank. Officially Valid Documents (OVD) are as under: a. Proof of Possession of Aadhaar Number b. Passport c. Driving License d. Voter's Identity Card issued by Election Commission of India e. Job Card issued by NREGA duly signed by an officer of the State Government f. Letter issued by the National Population Register containing details of name and address g. Any other document as notified by the Central Government in consultation with the Regulator. **Banks can use physical copy of the Aadhaar card as well as e-Aadhaar, 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 but without e- KYC based authentication for those customers who do not give a declaration that s/he is desirous of receiving her/his entitled benefits for subsidies welfare schemes funded from the Consolidated Fund of India in her/his account directly. **(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 26-09-2018).**
Accounts of Proprietorship Concerns	
Proof of name, address and activity of the concern	For Proprietary concerns, in addition to the PAN No and certified copy of documents applicable to the individual (proprietor), any two of the following documents in the name of the proprietary concern should be submitted: a. Registration certificate (in the case of a registered concern). b. Certificate / license issued by the municipal authorities under Shop and Establishment Act. c. Sales and income tax returns. d. CST/VAT/ GST certificate (provisional / final). e. Certificate / registration document issued by Sales Tax / Service Tax/Professional Tax authorities. f. 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.

	g. Utility bills such as electricity, water, landline telephone bills, etc h. 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. RBI vide its notifications dated 15.05.2004 and 02.07.2015 has instructed all Banks that at the time of opening of Current Accounts, Bank should insist on declaration from the account holder to the effect that he is not enjoying any credit facility with any other bank or obtain a declaration giving particulars of credit facilities enjoyed by the intending customer with any other bank(s). 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	
Proof of name, address and activity of the concern	Where the client is a partnership firm, certified copies of following documents or the equivalent e-documents of all the following documents are to be submitted: a. Registration Certificate b. Partnership Deed c. Permanent Account Number of the Partnership Firm d. a. Any Officially Valid Document which contains proof of identity/address in respects of managers, officers and employees holding an attorney to transacts on its behalf. And b. PANs 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 partnership firm. RBI vide its notifications dated 15.05.2004 and 02.07.2015 has instructed all Banks that at the time of opening of Current Accounts, Bank should insist on declaration from the account holder to the effect that he is not enjoying any credit facility with any other bank or obtain a declaration giving particulars of credit facilities enjoyed by the intending customer with any other bank(s). 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 companies	
Proof of name, address and activity of the concern	Where the client is a company, certified copies of documents or the equivalent e-documents of all the following documents are to be submitted: a. Certificate of incorporation b. Memorandum and Articles of Association c. Permanent Account Number of the Company d. A resolution from the Board of Directors and Power of Attorney granted to its managers, officers or employees to transact on its behalf. e. a. Any Certified Officially Valid Document which contains proof of identity / address in respects of managers, officers and employees holding an attorney to transact on its behalf. And b. PANs or Form 60/61 as defined in the Income Tax Rules, 1962 issued to managers, officers or employees holding an attorney to transact on the company's behalf. RBI vide its notifications dated 15.05.2004 and 02.07.2015 has instructed all Banks that at the time of opening of Current Accounts, Bank should insist on declaration from the account holder to the effect that he is not enjoying any credit facility with any other bank or

	obtain a declaration giving particulars of credit facilities enjoyed by the intending customer with any other bank(s). 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 trusts	
Proof of name, address and activity of the concern	Where the client is a Trust, certified copies of documents or the equivalent e-documents of all the following documents are to be submitted: a. Registration Certificate b. Trust Deed c. Permanent Account Number or Form 60/61 of the Trust d. a. Any Certified Officially Valid Document which contains proof of identity / address in respects of managers, officers and employees holding an attorney to transact on its behalf. And e. PANs 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 Trust.
Accounts of Unincorporated Association or body of individuals	
Proof of name, address and activity of the concern	Where the client 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: a. Resolution of the managing body of such association or body of

	individuals b. Permanent Account Number or Form 60/61 of the Unincorporated association or a body of individuals c. Power of Attorney granted to the person who will transact on its behalf. d. a. Any Certified Officially Valid Document which contains proof of identity/address in respects of managers, officers and employees holding an attorney to transact on its behalf. And e. a. 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 unincorporated association or a body of individuals.
accounts of Governments or its Departments, societies, universities and local bodies like village panchayats	
Proof of name, address and activity of the concern	i. Document showing name of the person authorized to act on behalf of the entity; a. 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. And b. 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.
Accounts of Limited Liability Partnerships	
Proof of name, address and activity of the concern	a. Certified copy of incorporation documents filed with registrar of Companies

	b. Certificate issued by the registrar of Companies c. Copy of LLP Agreement signed by all the parters. In case, there is no LLP Agreement, Schedule I of the LLP Act signed by all the partners will prevail. d. (i) Any Certified Officially Valid Document which contains proof of identity / address in respects of person holding an attorney to transacts on its behalf and (ii) PAN 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
Relaxation for Accounts of low risk customers	
'Simplified measures' may be applied in the case of 'Low risk' customers taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved.	Additional documents deemed to be certified OVDs for the purpose of proof of identity where simplified measures are applied: a. Identity card with applicant's photograph issued by Central /State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions; b. Letter issued by a gazetted officer, with a duly attested photograph of the person. For the limited purpose of proof of address, the following additional documents are deemed to be OVDs where simplified measures are applied: a. Utility bill which is not more than two months old of any service provider (electricity, telephone, postpaid mobile phone, piped gas, water bill);

	b. Property or Municipal Tax receipt; c. Bank account or Post Office saving bank account statement; d. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departmentsor Public Sector Undertakings, if they contain the address; e. Letter of allotment of accommodation from employer issued by Central / State Governmet departmens, Statutory or Regulatory bodies, Public Sector Undertakings, Scheduled Commercial Banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting officials accommodation; and f. Documents issued by Government departments of foreign jurisdiction and letter issued by Foreign Embassy or Mission in India.
Branches to obtain only the documents as mentioned above and not to accept any other document for KYC purpose.	

ANNEXURE – VII

KYC documents for eligible FPIs under PIS

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

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

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

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

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

ANNEXURE – VIII

Customer-Category-wise Threshold limits for per transactions as per Risk Category of the customer, type of account / product code of the account

Customer-Category-wise Threshold Limits for per transactions as per Risk Category of the customer, type of account / product code of the account					
ACCT TYPE	**INT CAT**	**Description**	**Risk Category**		
			Low	**Medium**	**High**
Savings					
2011	1401	SB-Chq General-Pub-IND-ALL	1,00,000	1,50,000	2,00,000
2011	2401	SB-Chq General-Pub-Oth-All	1,00,000	1,50,000	2,00,000
2011	3401	SB-Chq General-Staff-All	1,00,000	1,50,000	2,00,000
2011	6401	SB-Chq General-Trust-All	xxxx	xxxx	1,50,000
2013	1401	SB-Chq NRO-Pub- Ind-All INR	xxxx	xxxx	5,00,000
2014	1401	SB-Chq NRE-Pub- Ind-All INR	xxxx	xxxx	5,00,000
2017	1401	Sav-Chq-FGN-Nat-Pub-Ind-All INR	xxxx	xxxx	5,00,000
2020	1401	SB-Chq PENSN Pub-Ind-All INR	1,00,000	xxxx	xxxx
2020	3401	SB-Chq PENSN STFF Ind-All INR	1,00,000	xxxx	xxxx
2022	1401	SB-Maha Bank Lok Bachat Yojana	10,000	xxxx	xxxx
2023	1401	Sav-Chq-Yuva-Pub-Ind-All INR	50,000	xxxx	xxxx
2026	1401	SB-Salary Gain-Pub-Ind-All	1,00,000	xxxx	xxxx
2026	3401	SB-Salary Gain-STF-Ind-All	1,00,000	xxxx	xxxx
2029	1401	SB-Chq-Flexi -Pub- Ind-All-INR	2,00,000	xxxx	xxxx
2029	3401	SB-Chq-Flexi -Staff-All-INR	2,00,000	xxxx	xxxx
2030	3401	Sav-Chq-Flexi NRO-Stff-All-INR	xxxx	xxxx	10,00,000
2031	1401	Sav-Chq-Flexi-NRE-Pub-Ind-All	xxxx	xxxx	10,00,000
2033	1401	FI-Maha Bank Lok Bachat Yojana	10,000	xxxx	xxxx
2064	1401	Maha Suraksha Payroll-Comm Off	2,00,000	xxxx	xxxx
2065	1401	Maha Suraksha Payrol-BelCommOff	2,00,000	xxxx	xxxx
2090	3401	SB-CO-Chq-Gen-St-All	2,00,000	xxxx	xxxx
2090	6401	SB-CO-Chq-Gen-Trust-All	xxxx	xxxx	1,00,000
2111	1401	SB-W/oChq-Gen-Pub-Ind-All INR	1,00,000	1,50,000	2,00,000
2120	1401	SB-WChq-Pens-Pub-Ind-All INR	1,00,000	xxxx	xxxx
2122	1401	SB-MahaSetu-FI-W/oCHq-Pub_Ind	10,000	xxxx	xxxx
2123	1401	SB-w/o-Chq-Bk-YUVA-INSTACARD	10,000	xxxx	xxxx
2124	1401	SB-NSIGSESchoI-W/oCHq-Pub_Ind	10,000	xxxx	xxxx
2125	1401	SB-CapitalGain-Pub-Ind-All-INR	5,00,000	7,50,000	10,00,000
2125	2401	SB-CapitalGain-Pub-Oth-All-INR	5,00,000	7,50,000	10,00,000
2129	1401	SB-w/oFlexi -Pub- Ind-All-INR	1,00,000	1,50,000	2,00,000
2133	1401	SBFIMahaBank Schlrshp Minority	10,000	xxxx	xxxx
2311	1401	Mahabank CorpSUP Payroll Sch	2,00,000	xxxx	xxxx

2353	2401	SBChqMahabank Govt Zero Bal Sch	10,00,000	xxxx	xxxx
2058	1401	Mahabank Royal SB A/C	5,00,000	7,50,000	10,00,000
2059	1401	Maha Sarvjan SB A/C	10,000	xxxx	xxxx
2091	1401	Mahabank Puple SB A/C	5,00,000	7,50,000	10,00,000

ACCT TYPE	INT CAT	Description	Risk Category		
			Low	Medium	High
Current					
1011	1101	Cur-Gen-Pub-Ind-NonRural-INR	5,00,000	7,50,000	10,00,000
1011	1991	Cur-Gen-Pub-Ind-Rural-SU-INR	3,00,000	5,00,000	7,00,000
1011	2101	Cur-Gen-Pub-Corp-NonRural	10,00,000	15,00,000	25,00,000
1011	2991	Cur-Gen-Pub-Corp-oth-Rural-SU	5,00,000	7,50,000	10,00,000
1011	6401	Cur-Gen-Trusts-All-INR	xxxx	xxxx	5,00,000
1053	2401	Cur-Govt-Pub-Oth-AllINR	10,00,000	xxxx	xxxx
1054	2101	BOM e-PAYMENT OF TAX	xxxx	xxxx	xxxx
1057	1401	Cur-Diamond Pub-Ind-INR	5,00,000	7,50,000	10,00,000
1057	2401	Cur-Diamond Pub-Oth-INR	5,00,000	7,50,000	10,00,000
1511	2101	CUR-SPL-PUB-CORP-OTH-NRural	5,00,000	7,50,000	10,00,000

ANNEXURE – IX

Indicative Alert Indicators for Branches/ Departments to report suspicious transactions / attempted transactions

Alert indicator		Indicative rule / scenario
CV– Customer Verification		
CV1.1	Customer left without opening the account	Customer did not open the account after being informed about kyc
CV2.1	Customer offered forged or false documents	Customer gives false documents or documents that appear to be forged / inaccurate / altered
CV2.2	Documents are not verifiable	Documents for identification are not verifiable i.e. Foreign documents
CV 3.1	Address found to be non-existent	Address provided by customer found to be non-existent
CV 3.2	Address found to be wrong	Customer not staying at the address provided at the time of account opening
CV 4.1	Difficult to identify the beneficial owner	Customer uses complex legal structures
LQ- Law Enforcement Agency Query		
LQ 1.1	Customer being investigated for criminal offences	Customer has been the subject of inquiry from Any law enforcement agency relating to criminal offences
LQ 2.1	Customer being investigated for TF offences	Customer has been the subject of inquiry from Any law enforcement agency relating to criminal offences or TF offences
MR– Media Reports		
MR 1.1	Adverse media report about criminal activities customer	Match of customer details with persons reported in local media/ open source for criminal offences
MR 02.1	Adverse media report about terrorism finance activities customer	Match of customer details with persons reported in local media/ open source for criminal offences and TF activities
EI – Employee Initiated		
EI 1.1	Customer did not complete transaction	Customer did not complete transaction after queries such as source of funds
EI 2.1	Customer is nervous	Customer is hurried or nervous
EI 2.2	Customer is over cautious	Customer over cautious in explaining genuineness of transaction
EI 2.3	Customer provides inconsistent information	Customer provides information that seems false/minimal or inconsistent
EI 3.1	Customer acting on behalf of a third party	Customer has vague knowledge about amount of money involved in the transaction
EI 3.2	Multiple customers working as	Multiple customers arrive together but pretend

Alert indicator		Indicative rule / scenario
	a group	to ignore each other
EI4.1	Customer avoiding nearer	Customer travels unexplained distances to conduct transactions
EI 4.2	Customer offers different identification on different occasions	Customer offers different identification on different occasions with an apparent attempt to avoid linkage of transactions.
E14.3	Customer wants to avoid reporting	Customer wants to avoid reporting by convincing staff.
E14.4	Customer could not explain source of funds	Customer could not explain source of funds satisfactorily
E15.1	Transaction is unnecessarily complex	Transaction is unnecessarily complex for its stated purpose.
E15.2	Transaction has no economic rationale	The amounts or frequency or the stated reason of the transaction does not make sense
E15.3	Transaction inconsistent with business	Movement of transaction inconsistent with customer's business
E15.4	Unapproved inward remittance in NPO	Foreign remittance received by NPO not approved by FCRA
E17.1	Complaint received from public	Complaint received from public for abuse of account for committing fraud etc.
E18.1	Alert raised by agent	Alert raised by agents about suspicion.
E19.1	Alert raised by other institution	Alert raised by other institutions, subsidiaries or business associates including cross-border referrals.

ANNEXURE – X

Examples of STRs received At FIU-IND

Examples of STRs received At FIU-IND		
	Type of Suspicion	**Summary of Detection and Report**
1	False Identity	Identification documents found to be forged during customer verification process. The account holder not traceable.
2	Wrong Address	Welcome pack received back since the person was not staying at the given address. In some cases, the address details given by the account holder found to be false. The account holder not traceable.
3	Use of similar sounding corporate names	Account was opened with names very close to other established business entities.
4	Doubt over the real beneficiary of the account	Customer not aware of transactions in the account. Transactions inconsistent with customer's profile.
5	Account of persons under investigation	The customer reported in media for being under investigation/ Account of a customer frozen by the bank
6	Account of wanted criminal	Name of the account holder and additional criteria (Date of birth/Father's name/Nationality) matched with details on a Watch List of UN, Interpol etc.
7	Account used for cyber crime	Complaints of cybercrime received against a customer. The transactions in the account have no valid explanation.
8	Account used for lottery fraud	Complaints received against a bank account used for getting money deposited by victims No valid explanation for the transactions by account holder. Cash withdrawals using ATMs immediately after deposits.
9	Doubtful activity of account holder	Cash deposited in a bank account at multiple cities on the same day. The account holder a citizen of country with high rate of drug trafficking.
10	Doubtful investment in IPO	Large number of accounts involving common introducer or authorized signatory. Accounts used for multiple investments in IPOs of various companies.
11	Unexplained transfers between multiple accounts	Large number of related accounts with substantial inter-account transactions without any economic rationale.
12	Unexplained activity in dormant accounts	The customer could not provide satisfactory explanation to Transactions in a dormant account.
13	Suspicious cash withdrawals	Large value cheques deposited followed by immediate

	in bank account	cash withdrawals.
14	Doubtful source of foreign inward transfers in bank account	Deposit of series of demand drafts purchased from Exchange House abroad. Sudden deposits in dormant account immediately followed by withdrawals.
15	Doubtful remitter of foreign remittances	Name and other details of the remitter matches with a person on watch list
16	Doubtful utilization of Foreign remittances	Foreign remittance being withdrawn in cash immediately. No valid explanation
17	Misappropriation of funds	Reports of misappropriation of funds. Substantial cash withdrawals in account of a charitable organization
18	Unexplained activity in Account inconsistent With what would be expected from declared business	Transactions in account inconsistent with declared business. The Customer could not provide satisfactory explanation.
19	Unexplained large Value transactions inconsistent with client's Apparent financial standing	Large value transactions in an account usually having small Transactions without any economic rationale.
20	Doubtful source of payment for credit card purchases	Credit card topped up by substantial cash first and then used for incurring expenses. Cumulative payment during the year was beyond known sources of income.
21	Suspicious use of ATM card	Frequent cash deposits in the account followed by ATM withdrawals at different locations. No valid explanation.
22	Doubtful use of safe deposit Locker	Safe deposit locker operated frequently though the financial status of client does not warrant such frequency. Large suitcase brought by customer.
23	Doubtful source of cash deposited in bank account	Cash transactions of value just under the reporting threshold. Cash transactions spilt across accounts to avoid reporting. No valid explanation

ANNEXURE –XI

Additional Alert Scenarios for Identifying Suspicious Transactions Related to Trade Based Money Laundering

S. N.	ADDITIONAL ALERT SCENARIOS FOR IDENTIFYING SUSPICIOUS TRANSACTIONS RELATED TO TRADE BASED MONEY LAUNDERING
1	Scenarios for verifying the actual date of import and the date of remittance
2	Many proprietorship firms importing from the same exporter from a foreign land
3	Advance waivers provided or pre-accepted discrepancy by the applicant and/or the applicant is over keen to waive discrepancy
4	Representation of an official document immediately after a turn-down for discrepancy
5	Submission/payment of round figure bills
6	Transaction limits for the first time import active customer
7	Outward remittance to same overseas party (with internal thresholds for the number of days and number of transactions)
8	Outward remittance of same value from single customer. Mot\re than x transactions on last y days.
9	Cumulative transaction amount (frequency and the amount thresholds according to the bank's experience) in outward remittance.

*****