ORIENTAL BANK OF COMMERCE

Corporate Strategy & Planning Department Corporate Office : Gurugram

Oriental Bank of Commerce (OBC) - Policy on "Know Your Customer" (KYC) Norms and "Anti-Money Laundering" (AML) Measures : Operational Guidelines

Guidelines on **"Know Your Customer" (KYC) Norms** were last issued vide our Circular No. HO/CS&P/8/2018-19/219 dated 15th June, 2018. Further, the bank has issued various circulars for implementing the RBI guidelines on KYC/AML compliance from time to time.

The Reserve Bank of India vide their Master Direction No. DBR.AML.BC.No.81/14.01.001/2015-16 dated 25.02.2016 (Updated as on May 29, 2019) has updated the guidelines/ instructions on Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/ Obligation of banks under PMLA, 2002 .

The KYC/AML guidelines issued by RBI vide Master Direction No. DBR.AML.BC.No.81/14.01.001/2015-16 dated 25.02.2016 (Updated as on May 29, 2019) have been incorporated in this policy.

Application

i) **The instructions, contained in the master circular, are applicable to all Regulated Entities (REs).**

ii) These guidelines have been issued 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. Any contravention thereof or non-compliance shall attract penalties under Banking Regulation Act.

Purpose

Banks have been advised to follow certain customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority. These „Know Your Customer" guidelines have been revisited 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). Detailed guidelines based on the Recommendations of the Financial Action Task Force and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision, with indicative suggestions wherever considered necessary, have been issued. Banks have been advised to ensure that a proper policy framework on „Know Your Customer" and Anti-Money Laundering measures with the approval of the Board is formulated and put in place.

Accordingly the policy of the bank on KYC/ AML is revised / updated as follows:

Bank's KYC Policy Guidelines

1. **OBC 'Know Your Customer' Policy-(FY 2018-19 & onwards)**

1.1 KYC Norms/Anti Money Laundering (AML) Measures/Combating Financial Terrorism (CFT) Obligations of banks under PML Act, 2002

The objective of KYC/AML/CFT guidelines is to prevent bank from being used intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable banks understand their customers and their financial dealings better which in turn help them manage their risks prudently.

1.2 Definition of Customer

For the purpose of "KYC Policy", a 'Customer' has been defined as:

- a person or entity that maintains an account and/or has a business relationship with the bank;
- one on whose behalf the account is maintained (i.e. the beneficial owner);*
- beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
- any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

(*The beneficial owner means the natural person who ultimately owns or controls a client and or the person on whose behalf a transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person)

1.3 General Guidelines

i) The information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purpose and should be in conformity with the guidelines issued in this regard. Any other **Optional/additional** information from the customer should be sought separately with his/her consent and after opening the account.

ii) It should be ensured that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travelers' cheques and Transactions pertaining to Sale of gold/silver/platinum for value of Rupees fifty thousand and above is effected by debit to the customer's account or against cheques and not against cash payment.

Further, with effect from September 15, 2018, 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.

iii) It should be ensured that the provisions of Foreign Contribution (Regulation) Act, 1976 as amended from time to time, wherever applicable are strictly adhered to.

iv) w.e.f. April 1, 2012, banks should not make payment of cheques/drafts/pay orders/banker's cheques bearing that date or any subsequent date, if they are presented beyond the period of **three months** from the date of such instrument.
v) Introduction shall not be sought while opening accounts.

vi) 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

Secrecy Obligations and Sharing of Information:

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

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

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

i. Where disclosure is under compulsion of law,

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

iii. the interest of bank requires disclosure and

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

1.4 KYC Policy

a) Scope: Meeting the requirements of OBC 'KYC' Policy will always take precedence over all other aspects of managing customer relationships i.e. these policy guidelines shall be binding on all concerned in the bank for the opening of accounts, entering into customer / business relationships as well as for closure of the accounts of the customers / termination of customer / business relationships, as stated / enumerated in the following pages.

b) Policy Application: OBC 'KYC' Policy shall be applicable to the branches / subsidiaries outside India as well, i.e. as and when the bank opens any branch/(es) or any majority owned subsidiary located abroad, these guidelines shall also apply to the same, especially, in which do not or insufficiently apply the FATF recommendations, to the extent local laws permit. Wherever the local applicable laws and regulations prohibit implementation of these guidelines, the same shall be brought to the notice of Reserve Bank of India as directed

The bank's guidelines on Security Market Intermediaries under the Prevention of Money Laundering Act 2002 and rules and KYC/ AML/ CFT Guidelines for Money Transfer Service Scheme & Money Changing Activities also form part of this policy.

1.5 Key Definitions: Terms used in the Policy are defined as under:

Regulated Entities(REs) means

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

b. All India Financial Institutions (AIFIs)

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

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

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

Customer means a person who is engaged in a financial transaction or activity with a **Regulated Entity (RE**) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

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

Prospective Customer: A person or entity with which we intend to have an ongoing business relationship or a person or entity which has approached our bank for opening his account / entering into business relationship with our bank.
Customer Acceptance: The process by which a customer becomes a customer of OBC i.e. a prospective customer

shall become customer of OBC once the Customer Acceptance Policy / Procedures have been completed and the requirements of the relevant Category of the Customer standards met.
Customer Transaction Profile: A profile of customer expected transactions in the account, derived from the information gathered during the customer acceptance process and throughout the customer relationship.

Related Party: Any party associated with a customer i.e. customer's customer or customer to whom the requirements set forth in this Policy for acceptance of a customer must also be applied in order for the customer to be accepted.

Rejected Prospective Customer: A prospective customer for whom the requirements of the relevant KYC category for customer acceptance have not been met.

Mandatory Information: Customer information which is to be held to satisfy legal and statutory obligations and is not optional viz. identification, address and other mandatory information.

Optional Information: This is the information to be collected from prospective customer or customer with their sole and explicit consent only and after informing them about the purpose of collecting such information.

Threshold limit-Threshold limit means the annual credits expected in the account.

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

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

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

i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
ii. property or Municipal tax receipt;
iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;
c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above
d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.
Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

Person
In terms of PML Act a 'person' includes:
(i) an individual,
(ii) a Hindu undivided family,
(iii) a company,
(iv) a firm,
(v) an association of persons or a body of individuals, whether incorporated or not,
(vi) every artificial juridical person, not falling within any one of the above persons (i to v), and

(vii) any agency, office or branch owned or controlled by any of the above persons (i to vi).

-**Transaction**
"Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes -
opening of an account;
deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
the use of a safety deposit box or any other form of safe deposit;
entering into any fiduciary relationship;
any payment made or received in whole or in part of any contractual or other legal obligation; or
establishing or creating a legal person or legal arrangement.

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

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

Explanation- For the purpose of this sub-clause-

1. "Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.
2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.
b. Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.
c. Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

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

d. Where the customer is **a trust**, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

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

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

a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,
b. the Managing Partner, if the RE is a partnership firm,
c. the Proprietor, if the RE is a proprietorship concern,
d. the Managing Trustee, if the RE is a trust,
e. a person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and
f. a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks.
Explanation. - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.

Non-profit organisations (NPO) means any entity or organization 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.

Officially valid document(OVD) means the passport, the driving licence, the Permanent Account Number (PAN) Card, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.

Explanation: Customers, at their option, shall submit one of the six OVDs for proof of identity and proof of address.

Provided that where 'simplified measures' are applied for verifying the identity of the customers the following documents shall be deemed to be OVD:
identity card with applicant's photograph issued by Central/ State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
Letter issued by a Gazetted officer, with a duly attested photograph of the person.
Provided further that where 'simplified measures' are applied for verifying, for the limited purpose of, proof of address the following additional documents are deemed to be OVDs :
Utility bill, which is not more than two months old, of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
Property or Municipal Tax receipt;
Bank account or Post Office savings bank account statement;
Pension or family Pension Payment Orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and
Documents issued by Government departments of foreign jurisdictions or letter issued by Foreign Embassy or Mission in India.

Principal Officer means an officer nominated by the RE, responsible for furnishing information as per rule 8 of the Rules.

Suspicious transaction means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith,:
a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to not have economic rationale or bona-fide purpose; or
d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

A A Small Account' means a savings account **which is opened in terms of sub-rule (5) of the PML Rules, 2005.** In which:
a. the aggregate of all credits in a financial year does not exceed rupees one lakh;
b. the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and
c. the balance at any point of time does not exceed rupees fifty thousand.

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

Common Reporting Standards (CRS) means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

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

Customer identification means undertaking the process of CDD.

FATCA means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

"IGA" means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.

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

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

"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.

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

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

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

"Wire transfer" means a transaction carried out, directly or through a chain of transfers, on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank.

"Domestic and cross-border wire transfer": When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the 'originator bank' or 'beneficiary bank' is located in different countries such a transaction is cross-border wire transfer

Certified Copy of OVD- Obtaining a certified copy by regulated entity shall mean comparing the copy of officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the regulated entity.
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 of OVD, certified by any one of the following, may be obtained:

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

Offline Verification as defined in the Aadhaar and Other Law (Amendment) Ordinance, 2019, means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by the Aadhaar regulations.

Aadhaar number as defined in the Aadhaar and Other Law (Amendment) Ordinance, 2019, means an identification number issued to an individual under sub-section (3) of section 3 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), and includes any alternative virtual identity generated under sub-section (4) of that section.

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

""Authentication" means the process by which the Aadhaar number alongwith demographic information or biometric information of an individual is submitted to Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it."

1 Customers of Oriental Bank of Commerce: Customers of Oriental Bank of Commerce can be individuals and entities viz. Individuals (Indian national resident and non-resident) and entities viz. Organizations, Institutions, Companies, Firms, Trusts, Charities, NGOs, HUFs as well as Non-face to face customers. Further business relationships would include Correspondents etc. Branches to clearly spelt out the circumstances under which customer is permitted to act on behalf of another person/entity. 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.

1.1 In accordance with the broad regulatory guidance, the existing and the prospective customers shall be grouped based mainly on their social and financial status, nature of business activity, location of customer and clients, mode of payments, turnover volume, ability to confirm identity documents through online or other services offered by issuing authorities etc. to enable categorization of customers into low, medium, high and very high risk ones and KYC procedures shall be applied accordingly. Such risk based approach is considered necessary to avoid disproportionate cost to the bank and a burdensome regime for the customer as the nature of information/documents required would also depend on the risk perceived/type of customer.

2. "OBC Customer Identification Procedure (CIP)"

Customer Identification: In line with the directives / guidelines of the Govt. / Regulator, from time to time, banks have so far been satisfying themselves by obtaining and keeping on record the prescribed / directed documents from the customers and relying on the same for identity and address proof for opening new accounts. Reserve Bank of India has now advised that, being satisfied means that the bank must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Customer Identification has now been defined as identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information.. Bank shall carry out customer identification for a person who is not an account holder of the bank for any international money transfer operations. Decision-making functions of determining compliance with KYC norms shall not be outsourced.

Accordingly, necessary documents / information for establishing identity of each new customer, whether regular or occasional, as well as the purpose of the intended nature of banking relationship shall have to be ascertained. 'OBC Customer Identification Procedure (CIP)' has been worked out in this direction, which is risk perception based and shall be carried out at three stages viz.:

- While establishing a banking relationship i.e. during the process of opening of new account / establishing banking relationship;
- Carrying out a financial transaction; or
- When the bank has a doubt about the authenticity / veracity or the adequacy of the previously obtained customer identification data.

3.1 OBC Customer Identification Procedure (OBC CIP): 'OBC CIP' shall include obtaining all mandatory documents, identity and residence proofs i.e. as per the guidelines in vogue for opening new accounts of natural as well as legal persons, reliable and independent source documents, data, information and interviewing of the potential customers for ascertaining, verifying and establishing identity of prospective customers along with the purpose of intended customer relationship, sources of funds and threshold limits. Similar procedure shall be followed in case of existing customers as well in line with the perceived risk or where there is any doubt about the veracity of documents / information / data earlier provided by the customer. Branches shall carry **Customer due diligence (CDD)** in identifying and verifying prospective customers, detailed as under:

Customer Due Diligence (CDD) Procedure in case of Individuals:-

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

(a) a certified copy of any OVD containing details of his identity and address

(b) one recent photograph

(c) the Permanent Account Number or Form No. 60 as defined in Income-tax Rules, 1962, and

(d) such other documents pertaining to the nature of his/her business or financial status.

Provided that,
i) Aadhaar number from an individual, who is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and

Services) Act, 2016 (18 of 2016), shall be obtained. On receipt of the Aadhaar number from the customer, authentication of the customer's Aadhaar number may be carried out using e-KYC authentication facility provided by the Unique Identification Authority of India upon receipt of the customer's declaration that he/ she is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 (18 of 2016) in his/ her account.

ii) Aadhaar authentication/ offline-verification may be carried out in case of an individual who voluntarily uses his Aadhaar number for identification purpose.

In cases where successful authentication has been carried out, other OVD and photograph need not be submitted by the customer.

Provided further that in case biometric e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, Bank shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD from the customer. CDD done in this manner shall invariably be carried out by an official of the Bank and such exception handling shall also be a part of the concurrent audit. Bank shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Bank and shall be available for supervisory review.

Explanation 1: Bank shall, where its customer submits his Aadhaar number, ensure such customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act.

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

3.1.1 Documents / Information: As per existing guidelines a prospective customer, for opening of account **individually as well as jointly**, completes following formalities and provides documents as per the RBI directions or mandated by law / Govt.

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

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

3.1.1.3 Indicate mode of operation.

3.1.1.4 Avail of the nomination facility in case of individual accounts

3.1.1.5 Provide documents for identification and proof of residence - Particulars of either present or permanent addresses along with telephone numbers, if installed. **The customers shall not be required to furnish an additional OVD, if the OVD submitted by the customer for KYC contains both proof of identity and proof of address. A copy of the 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 shall be obtained for proof of address and identity, while establishing an account based relationship or while undertaking periodic updation exercise in cases of persons who change their names on account of marriage or otherwise**

<u>Explanation</u>: Customers, at their option, shall submit one of the six OVDs for proof of identity and proof of address.

3.1.1.6 Give details of other accounts with any other banks (for Current Accounts)

3.1.1.7 Permanent Account Number (PAN) given by Income Tax authorities or declarations as applicable.

3.1.1.8 Documents pertaining to the nature of business or financial status specified by the bank in policy. For example- Registration certificate; Partnership deed; and An officially valid document in respect of the person holding an attorney to transact on its behalf; for accounts of Partnership firms and Certificate of incorporation; Memorandum and Articles of Association; A resolution

from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf; for accounts of companies.

Document required for different Customer Groups have been given in Annexure I

The above documents / data would help to establish the identity of most of the prospective customers, but will not be sufficient to, i either ascertain and establish identity or / and location or / and sources of funds of those prospective customers who provide fabricated documents or are perceived to be of high / very high risk, where intensive kind of customer due diligence is required

ii. Prepare a profile of expected activities in the account, for which additional details need to be collected.

KYC documents required for opening accounts of Non Residents are Annexed I (a)

3.1.2 Verification of Identity / Identification of a customer is important pre-requisite for opening an account. No Account should be opened for any customer without proper verification of the identity of the person.

Identity: A person may be a natural or legal person, which are defined as under:

(a) Natural Person: A natural person's identity comprises his name and all other names used, date of birth, and an address at which he/she can be located.

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

Verification of Identity: Identification is the act of establishing who a person is. In the context of KYC, identification means establishing who a person purports to be. Verification of identity is the process of proving whether a person actually is who he claims to be. In the context KYC, verification is the process of seeking satisfactory evidence of the identity of those with whom the bank does business or intends to do business.

As a second step of applying KYC Procedure – Checking correctness of documents / information provided by the Prospective Customer: Verification of Identity can be done by carrying out checks on the correctness / veracity of the information / documents provided by the prospective customer or customer. Verification of Identity by checking veracity of information / documents is necessary in cases mentioned under 3.1.1.i and would constitute part of the intensive due diligence required in such cases.

In such cases, the best available evidence of identity should be obtained, i.e. having regard to the circumstances of each prospective customer as some forms of proof of identity are more reliable than others and in some cases it will be prudent to carry out more than one verification check, which should be documented while verifying the identity of the prospective customer.

Documents (OVDs) to be obtained for establishing identity of a person are:

- Valid Passport,
- Valid Driving License,
- Valid **proof of possession of Aadhaar number**,
- Valid Voter's Identity Card issued by the Election Commission of India,
- Job card issued by NREGA duly signed by an officer of the State Government and
- **Letter issued by the National Population Register containing details of name and address.**

These are the documents on the basis of which Identity of a customer can be established and in case of need correctness of these documents can be ascertained by accessing databases (wherever available) or from the issuing offices and identity verified.

Rule 114B of Income Tax Rules: Quoting of PAN: Verification of details furnished by the Customer: Quoting of PAN is mandatory for opening bank accounts, placing fixed deposits in excess of Rs. 50000/- depositing Rs. 50000/- or more in Cash to a bank account on any day, issue of demand drafts against payment of cash of Rs. 50000/- or more, issue of credit cards, etc under Rule 114B of Income Tax Rules. Banks are required to verify the PAN quoted by the customers.(account based as well as walk-in customers)

Bank has started online real time verification of the customer's PAN number before accepting the PAN of the customer

and/or effecting any transaction. (link on OBCWEB http://172.16.200.10/obcweb/)

PAN of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B applicable to banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN.

A list of the nature and type of documents/ information that may be relied upon for customer identification is given in **Annexure I (for resident) & I(a) (for Non-resident)** to this circular. The permanent correct address means the address at which a person usually resides. Henceforth only one documentary proof of address (either current or permanent) may be obtained from the customers while opening a bank account or while undergoing periodic updation. In case the address mentioned as per 'proof of address' undergoes a change, fresh proof of address may be submitted to the branch within a period of six months.

Mobile number for opening account has been made mandatory.

For opening of Resident Individual account, name as spelt on Officially Valid Document (OVD) used as identity document shall be accepted.

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

OTP based e-KYC

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.

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

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

(v) Accounts, both deposit and borrowal, opened using OTP based e-KYC shall not be allowed for more than one year within which Customer Due Diligence (CDD) procedure is to be completed. If the CDD procedure is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no further debits shall be allowed.

(vi) **A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other regulated entity.**
Further, while uploading KYC information to CKYCR, Bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other regulated entities shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

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

3.1.3 For customers that are legal persons or entities, branches should

- verify the legal status of the legal person / entity through proper and relevant documents;
- verify that any person purporting to act on behalf of the legal person / entity is so authorized and identify and verify the identity of that person; and
- understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

3.1.3.1 Identification of Beneficial Owners:
The branches should take reasonable a measure to identify the owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner/s is/are.

The term 'beneficial owner' has been defined as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person.**. The revised procedure as advised by the RBI 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 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.

3.1.3.2 Unique Customer identification code

The increasing complexity and volume of financial transactions necessitate that customers do not have multiple identities within a bank, across the banking system, across the financial system. This can be achieved by introducing a Unique Customer Identification Code.(UCIC) for each customer. This will help bank to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable bank to have a better approach to risk profiling of customers.
The finacle system is enabled for maintaining the uniformity of customer ID and guidelines are already in place.(HO Cir: HO/I&C/KYC-AML/2012-13/257 dated 12.07.2012)

Branches shall ensure that there is only one customer ID for one customer in the bank.

3.1.3.3 Intra bank Transfer of Accounts

When customers approach branch for transferring their account from one branch of the bank to another branch it is advised that KYC once done by one branch of the bank should be valid for transfer of the account within the bank as long as full KYC has been done **and the same is not due for periodic updation** for the concerned account**.** The customer should be allowed to transfer his account from one branch to another branch without restrictions.

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

B) In case the proof of address furnished by the customer is not the local address or address where the customer is currently residing, the branch may take a declaration of the local address on which all correspondence will be made by the branch with the customer. No proof is required to be submitted for such address for correspondence/local address. However, this address shall be verified by the branch.

3.1.3.4 Opening Accounts of self Help Groups

While opening the accounts of SHGs and credit linking their accounts, KYC verification of all the members of SHGs need not be done. KYC verification of all the office bearers would suffice. At the time of credit liking, no separate KYC verification of the members or office bearers is necessary (ref: DBOD.AML.BC.No.65/14.01.001/2012-13 dated 10.12.2012)

3.1.4 Customer Identification requirements-Indicative Guidelines

When there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or 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 the business relationship.

In cases as mentioned under **3.1.1** besides measures for verifying the identity and location of the prospective and the existing customers as mentioned in the preceding pages, intensive customer due diligence is to be carried as well as additional documents and information be gathered so as to ascertain the actual purpose of opening account with the bank, identities of all the persons, some of the examples are given as under :

3.1.4.1 Accounts of Companies and Firms: Branches / offices need to be more vigilant against business entities, which are being used by individuals as a 'front' for maintaining accounts with the banks. Intense due diligence is to observed, specifically in case of companies having close family shareholding or beneficial ownership or firms with sleeping partners etc. Accordingly, in case of Companies and Firms additional information should be gathered and examined as regards:

- Control structure of the entity;
- Source of funds;
- Identify all the natural persons who have a controlling interest; and
- Who comprise the management?

Such information shall be the part of the Profile and basis for the customer acceptance in case of the prospective customers i.e. depending upon the risk perception. These requirements can 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.

KYC documents required for private limited company constituted under OPC(one person company) will remain same as are for other private limited companies except that in case of OPC, KYC documents of nominee as per memorandum of company be also obtained by branch.

3.1.4.2 Trust / Nominee or Fiduciary Accounts: There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. In such cases Branches shall determine,

- Whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary.
- In case of yes, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, and also details of the nature of the trust or other arrangements in place be insisted upon.
- The different categories of beneficiaries should be identified as defined in Para 3.1.3.1

In the case of a 'foundation', steps should be taken to verify the founder managers / directors and the beneficiaries, if defined

Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'

3.1.4.3 Client accounts opened by Professional Intermediaries:

- When the branch has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified.
- Branches may be holding 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Branches, however, shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the banks. Where funds held by the intermediaries are not co-mingled at the branch and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the branch, the branch shall still look into the beneficial owners.

Where the branches rely on the 'customer due diligence' (CDD) done by an intermediary, they shall satisfy themselves that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers. It should be understood that the ultimate responsibility for knowing the customer lies with the bank

3.1.4.4 Opening of Bank Accounts - Salaried Employees

In case of salary employed, it is clarified that with a view to containing the risk of fraud banks need to rely on such certification only from corporates and other entities of repute. The branches should be aware of the competent authority designated by the concerned employer to issue such certificate/letter. Further, **in addition** to the certificate from employer, branches should insist on **documents as specified in Customer Due Diligence (CDD) Procedure applicable for individuals** for KYC purposes for opening bank account of salaried employees of corporates and other entities.

3.1.4.5 Accounts of non-face-to-face customers

With the introduction of telephone and electronic banking, increasingly accounts are being opened for customers without the need for the customer to visit the bank branch. In such cases, branches may also require the first payment to be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the branch may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

3.1.4.6 Accounts of proprietary concerns

For opening an account in the name of a sole proprietary firm, **Customer Due Diligence (CDD) of the individual (proprietor),** as mentioned in Annexure-1, containing details of identity and address of the individual (proprietor) shall be obtained.

a. Registration certificate
b. Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
c. Sales and income tax returns.
d. **CST/VAT/GST certificate (provisional/final).**
e. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.
f. IEC(importer exporter code) issued to the proprietary concern by the office of DGFT/Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
g. Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.
h. Utility bills such as electricity, water, and landline telephone bills.

In cases where the Bank is satisfied that it is not possible to furnish two such documents, Bank at their discretion, accept only one of those documents as proof of business/activity .Bank shall undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

For opening accounts of juridical persons not specifically covered in the earlier part, such as Government or its Departments, societies, universities and local bodies like village panchayats,

One certified copy of the following documents shall be obtained.:
i. Document showing name of the person authorised to act on behalf of the entity;

ii. Officially valid documents for proof of identity and address in respect of the person holding an attorney to transact on its behalf and

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

3.1.4.7 Procedure to be followed in respect of foreign students:

The following procedure for foreign students studying in India shall be adopted.
i) 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.
ii) Branches shall obtain a declaration about the local address within a period of 30 days of opening the account and verify the said local address.
iii) During the 30 days period, the account shall be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of monthly withdrawal to Rs. 50,000/-, pending verification of address.
iv) The account shall be treated as a normal NRO account, and will be operated in terms of instructions contained in the Reserve Bank of India instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of Schedule 3 of FEMA Notification 5/2000 RB dated May 3, 2000.
v) Students with Pakistani and Bangladesh nationality will need prior approval of the Reserve Bank for opening the account.

3.1.4.8 Walk-in Customers

In case of transactions carried out by a non-account based customer, that is 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 should be verified. However, if a bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000/- the bank should verify identity and address of the customer and also consider filing a suspicious transaction report (STR) to FIU-IND.

NOTE: In terms of Clause (b) (ii) of sub-Rule (1) of Rule 9 of the PML Rules, 2005 banks and financial institutions are required to verify the identity of the customers for all international money transfer operations.

In case of cash transactions below Rs.50,000/- carried out by a non-account based customer that is walk-in-customer, full details of the customer, including complete address, telephone number etc, should necessarily be obtained and it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

Issue of demand draft, mail transfer, telegraphic transfer, NEFT/ IMPS ,any other mode or traveller cheque, and transactions pertaining to sale of gold/silver etc for Rs. 50,000 and above should be only by debit to the customer's account or against cheques or other instruments tendered by the purchaser and not against cash payment.

3.1.4.9 Politically Exposed Persons (PEPs) resident outside India:

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

- Sufficient information on PEPs intending to establish a relationship shall be gathered and information available on the person in the

public domain checked before accepting the PEP as a customer

- Identity of the person shall be verified and information sought about the sources of funds.
- Decision to open an account for PEP shall be taken at Head Office (CS&P Deptt) only.
- Accounts of PEPs if any shall be subject to enhanced monitoring on an ongoing basis.
- Above norms shall also be applied to the accounts of the family members or close relatives of PEPs.

Detailed guidelines on CDD measures to be made applicable to Politically Exposed Person (PEP) and their family members or close relatives are contained as above. It is further advised that in the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, branches should obtain senior management approval to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

These instructions shall also be applicable to accounts where a PEP is the beneficial owner.

3.1.4.10 Small Account

In case an individual customer who does not possess either any of the OVDs or the documents applicable in respect of simplified procedure and desires to open a bank account, banks shall open a 'Small Account', subject to the following:

a. The bank shall obtain a self-attested photograph from the customer.
b. The designated officer of the bank certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.
c. Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account.
d. Banks shall ensure that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place.
e. The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, the identity of the customer shall be established through the production of "officially valid documents".
f. Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established through the production of "officially valid documents".
g. The account remains operational initially for a period of twelve months which can be extended for a further period of twelve months, provided the account holder applies and furnishes evidence of having applied for any of the OVDs during the first twelve months of the opening of the said account.
h. The entire relaxation provisions shall be reviewed after twenty four months.

a) **A Small Account' means a savings account which is opened in terms of sub-rule (5) of the PML Rules, 2005.**

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

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

b) Rule (2A) of the Notification lays down the detailed procedure for opening 'small accounts'. Branches are advised to ensure adherence to the procedure provided in the Rules for opening of small accounts.

Officially Valid Documents

a) The Notification has also expanded the definition of 'officially valid document' as contained in clause (d) of Rule 2(1) of the PML Rules to include job card issued by NREGA duly signed by an officer of the State Government or the letters issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.
b) Accordingly, all accounts opened in terms of procedure prescribed in Rule 2A of the Notification dated December 16,

2010 referred to above should be treated as "small accounts" and be subject to the conditions stipulated in clause (i) to (v) of the sub-rule (2A) of Rule 9.
c) Banks may accept NREGA job card as "an officially document" for opening of bank account without the limitations applicable to "small accounts"
d) While opening accounts based on Aadhaar also, if the address provided by the account holder is the same as that on Aadhaar letter, it may be accepted as a proof of both identity and address.

3.1.4.11 Accounts of migratory workers

Ministry of finance vide notification No. 31/03/2011-BO II dated 28.12.2011 issued guidelines for opening accounts of migratory workers who have no proof of current place of residence. A migratory worker may visit any branch of the bank servicing the area of his/her residence native place) for opening the account. The branch will open his/her account on self certification basis, and/or on the basis of documents made available by the individual including a proof of permanent place of residence as the case may be, and allow operations immediately. The branch opening such an account may get the details/proof of permanent place of residence verified through an on line (Through e-mail) communication to the branch of the bank servicing the area of permanent domicile of the customer, within 30 days of opening of an account, within which the customer may be allowed operations as permissible for **small account** to enable him/her to meet basic day-to-day requirement of funds.

3.1.4.12 Selling Third Party Products

When bank sells third party products as agents, 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, bank shall follow the instructions of RBI given below:
a) Even while selling third party products as agents, bank shall verify the identity and address of the walk-in customer.
b) Bank shall also maintain transaction details with regard to sale of third party products and related records for a period and in the manner prescribed for our own products.
c) Banks' AML software shall be able to capture, generate and analyze alerts for the purpose of filing CTR / STR in respect of transactions relating to third party products with customers including walk-in customers.
d) The instructions/guidelines to make payment by debit to customers' accounts or against cheques for remittance of funds / issue of travelers' cheques, sale of gold / silver / platinum and the requirement of quoting PAN number for transactions of Rs.50,000 and above would also be applicable to sale of third party products by branches as agents to customers, including walk-in customers.

All the guidelines in respect of third party products would also apply to sale of banks' own products, payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product above the threshold of Rs.50,000/-.
All the guidelines in respect of third party products would also apply to sale of banks' own products, payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product above the threshold of Rs.50,000/-.

3.1.4.13 Reliance on third party due diligence:
For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Regulated Entities (REs), shall at their option, rely on customer due diligence done by a third party, subject to the following conditions:
(a) Records or the information of the customer due diligence carried out by the third party is obtained **within two days from the third party or from the Central KYC Records Registry.**
(b) Adequate steps are taken by Regulated Entities (REs) to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
(C)The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
(d) The third party shall not be based in a country or jurisdiction assessed as high risk.
(e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the RE.

3.1.4.14 Operation of bank accounts & money mules

a) "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."

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

c) The operations of such mule accounts can be minimized if branches follow the guidelines on opening of accounts and monitoring of transactions. Branches are, therefore, advised to strictly adhere to the guidelines on KYC/AML/CFT issued from time to time and to those relating to periodical updation of customer identification data after the account is opened and also to monitoring of transactions in order to protect themselves and their customers from misuse by such fraudsters.

3.1.4.15 At-par cheque facility availed by co-operative banks

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

3.1.4.15 Bank no longer knows the true identity

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

3.1.5 Additional Information for Customer Profile: It is mentioned under **3.1.1.ii** that basic information gathered for establishing or verifying identity is not sufficient to prepare a profile of expected activities in the account, for which additional details need to be collected, as under:

i) Employment details such as job specifications, salary structure, name and address of the employer, length of service, etc;
ii) Business details including details regarding clients and suppliers, their addresses;
iii) Details about source/sources of income and annual income;
iv) Details of assets owned such as house, vehicle etc.;

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

3.1.5 Customer Profile: As already mentioned under **2.7** Customer profile shall be prepared in case of all new accounts and in case of existing accounts depending on the risk perceived / category of the customer, as covered in detail in preceding pages. Besides basic information, the Profile shall also contain specific risk based information on points as mentioned under:

3.1.5.1 The profile shall be prepared by the official opening the account based on data / information provided by the prospective customer in account opening form, documents submitted, additional information gathered / furnished / collected through a structured interview.

3.1.5.2 A profile would give information / idea as to what type of transactions / activities to expect in the account, which is valuable for monitoring activities in the account.

3.1.5.3 Based on this information, the official shall fix the threshold limit for monitoring transactions in the account i.e. in case the threshold limit is to be fixed below the directed ones; otherwise the directed ones only will be fixed.

3.1.5.4 In case transactions are noticed in variance with the profile or do not match the customer profile, the account holder will be contacted for further details to the satisfaction of the branch. If required, profile shall be revised to reflect any change in the status.

3.1.5.5 The profile shall also help in evaluating the risk perception from the money laundering point of view. As already mentioned, based on the assessment, the account can be classified into "high risk"; "low risk" categories and this would determine the nature and extent of monitoring required.

3.1.5.6 Ongoing monitoring of transactions in the account and the level of their conforming to the customer / transaction profile etc can lead to review of the risk perception of an account i.e a low/Medium risk account can migrate to high risk one or a high risk one to low/Medium risk. However, the monitoring level will remain same.

3.1.5.7 Updation of customer identification data:

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

b) Full KYC exercise will be required to be done at least every two years for high risk individuals and entities.

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

.

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

Periodic updation shall be carried out as per the following procedure:

(a) Bank shall carry out:

i. Customer Due Diligence (CDD) Procedure (as mentioned in Annexure-1), at the time of periodic updation. However, in case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.

ii. In case of Legal entities, Bank shall review the documents sought at the time of opening of account and obtain fresh certified copies.

(b) Bank may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication/Offline Verification unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, OVD/Consent forwarded by the customer through mail/post, etc., shall be acceptable.

(c) Bank shall ensure to provide acknowledgment with date of having performed KYC updation.

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

In case of existing customers, Bank shall obtain **the Permanent Account Number 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 Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the Bank shall give the client an accessible notice and a reasonable opportunity to be heard.

Further, In case of existing 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, respective **Circle Head (in case of Udbhav/ Classic/ MCB-Classic Branches)** and **LCB/MCB Branch Head (in case of LCB/MCB Branches)** shall be competent authority to allow the operation in accounts of such customers. Such accounts shall, however, be subject to enhanced monitoring.

Provided further that if a customer having an existing account-based relationship with a Bank 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.
Explanation – For the purpose of this Section, "temporary ceasing of operations" in relation an account shall mean the temporary suspension of all transactions or activities in relation to that account by the Bank till such time the customer complies with the provisions of this Section. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

In case of higher risk perception on a customer review of risk categorization of customers, should be carried out at a periodicity of not less than once in six months.

Full KYC measures including meeting customers face to face: While implementing full KYC for non- resident customers the procedures outlined in our instructions on non-face to face customers para 3.1.4.5 may be adopted.
All Customers (all risk category) shall comply with full KYC requirements by visiting the base branch only.

d) Fresh photographs is required to be obtained from minor customer on becoming major.
e) Asset Accounts: KYC requirements and periodical updation thereof form part of AML/CFT guidelines and are applicable to asset side (Loan and Advances) customers also.
(RBI Letter No. DBOD.AML.BC.No.29/14.01.001/2013-14 dated July 12, 2013, RBI letter No DBOD.AML.No.5011/14.05.001/2013-14 dated 20.09.2013,RBI Cir. No. RBI/2013-14/150 DBOD.AML.BC.No.34/14.01.001/2013-14 dated 23.07.2013)

3.1.5.8. Threshold limit

Threshold limit means the annual credits expected in the account. It should not be confused with turnover i.e. total of credits and debits in the account. Fixing of threshold limit is very important and shall be based on profile of the customer. It is important to interview the customer by a senior official to understand the nature of business activity and the likely turnover in the account. Necessary information / documents regarding expected turnover must be collected. Then only the threshold limit can be fixed.

Threshold limit to be fixed should be in agreement with the risk profile of the customer and the business activity he is involved. However, threshold limit for small account shall be Rs. 1.00 Lac only. Threshold limits shall be reviewed as and when the breaches are observed and can be reviewed after getting additional information.

Threshold limit is to be based on the customer profile and the economic activity the person/ entity is engaged to ensure that the customer accounts are put to use for only for transactions related to his confirmed line of activity. Branch Incumbents must ensure that the interview of customers is focused on collecting the vital information for proper profiling of the customers. Documents evidencing his activities/ sources of funds must form the basis for fixing the threshold limit. In case of low risk category efforts should be made to collect the relevant information from available sources. Specific threshold limit should be fixed for each customer so that the tracking of the same is made effective. Based on this information, the official shall fix the threshold limit for monitoring transactions in the account.

On the basis of the background of the customers such as the country of origin, sources of funds, type of transactions involved, risk factors i.e. on the basis of
information gathered and compiled in customer profile, indicators need to be set for such type of accounts i.e. threshold limits should be fixed for monitoring transactions in such accounts.

A.FIXING OF THRESHOLD LIMIT- FOR INDIVIDUALS

Category(C1) Low Risk i.e. all salaried class, small and petty businessmen, pensioners, persons falling under Basic Saving Bank Deposit Account/Small account category, beneficiaries of Govt. Scheme loans etc. the policy prescribes that in all such cases the threshold limit be fixed as explained above. It is not proper to fix threshold limit based on only annual salary income. An individual is entitled to have all his personal transactions routed through the account which may also include small investments, loans and other small credits.

Professionals & highly paid employees-C2 -Medium Risk
Information should be gathered from the customer about the likely turnover, sources of income etc. before arriving at any Threshold Limit. In the normal course limit in excess of Rs.50 lacs shall be considered only on being satisfied

about the information provided by the customer.

High net worth individuals / non residents-C3-High Risk
High net worth individuals are from mainly business and industry backgrounds. Branches should correctly identify them and their correct profile giving the source of income and funds shall be recorded. These customers having high net worth, their accounts can reflect their personal transactions, investments, etc. however large volume of transactions with associate firms without any apparent purpose cannot be put through personal savings account. Savings accounts are meant for personal transactions only. Threshold limits over Rs. One crore can be fixed only when the branch is satisfied about the transactions. Sources of funds in case of non-residents cannot be easily identified.

However it must be ensured that the remittances received represents funds of the account holder and is used for personal purpose. If the requirement of threshold limit is huge and over Rs. One crore then more details shall be collected to satisfy the genuineness of the transactions.

PEPs of foreign origin and Persons of dubious reputation-C4-Very High Risk
Branches shall not open accounts under this category as it requires approval of head office as per policy.

B.FIXING OF THRESHOLD LIMIT - FOR OTHER THAN INDIVIDUALS
C1- Low Risk- all Govt Departments, Public Sector Undertakings, Statutory Bodies, Regulators.
These accounts are low risk accounts and threshold limit can be fixed on the basis of information provided by them. There need to be no restriction in fixing threshold limit of any amount. It must be noted that normally no current accounts of any business firms other than the above category can fall under low risk category.

C2 –Medium Risk- Private Organizations, Private Institutions, Public Limited Companies, Private Limited Companies, Firms (proprietary/partnership)
These can be classified as medium risk when identify and sources of funds is clearly established. Threshold limit be fixed after getting the information from the customer. Information like past turnover in the account for an existing account can be considered. Audited balance sheet of the business entity, tax returns, and other bank statements can be verified.

For any proprietary and partnership firms, threshold limit over Rs. One crore can be considered only when justified by the information collected. For any private limited company, Private Organizations, Private Institutions threshold limit over Rs. 5 crore shall be considered only when justified by information collected. For any public limited company threshold limit in excess of Rs.25 crores shall be considered only when justified by information collected.

C3 – High Risk- Private Organizations, Private Institutions, Public Limited Companies, Private Limited Companies, Firms (proprietary/partnership) (If sources of funds are not clear)

Threshold limit as in C2 above can be fixed but details must be collected for doing it.

C4 - Very High Risk -Companies having Close Family Shareholding or Beneficial Ownership Firms with Sleeping Partners- Trusts, Charities, NGOs and Organizations receiving Donations, All Non-face-to-face Customers

These are very high risk customers and come directly under the ambit of provisions of PMLA and CFT. Extra precautions shall have to be taken while opening the accounts under this category and fixing threshold limit shall be done after due diligence. ***Threshold limit of over Rs. One crore shall be fixed by the branch only when absolutely clear about the constitution, funding and purpose of these entities.***

4.Monitoring of Transactions

Definition of transaction:
"Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes -
i) opening of an account;
ii) deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment

order or other instruments or by electronic or other non-physical means;
iii) the use of a safety deposit box or any other form of safe deposit;
iv) entering into any fiduciary relationship;
v) any payment made or received in whole or in part of any contractual or other legal obligation;
vi) any payment made in respect of playing games of chance for cash or kind including such activities associated with casino; and
viii) Establishing or creating a legal person or legal arrangement.

Ongoing monitoring is the essential element of effective KYC procedures and by understanding the normal and reasonable activity of the customer, transactions falling outside the regular pattern can be easily identified and risk reduced effectively. However, the extent of monitoring will depend on the risk sensitivity of the account, which can be perceived during the initial phase of acceptance of customer and preparing the profile correctly. **Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored**

4.1 Branches need to pay special attention to all **Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose** and are in no conformity with the recorded customer profile .

4.2 Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer **,Transactions which exceed the thresholds prescribed for specific categories of accounts, Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts** should attract the attention of the branch

4.3 Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account.

There are indicators where suspicion may arise, can only be observed at the branches.(Ref:Cir HO/I&C/KYC/AML/51/2011-12/525 dated 25.10.2011, enlisting the different scenarios for identifying suspicious activities/transactions as formulated by IBA. An indicative list of Alerts & and indicative Rules/scenarios drawn by IBA is given in **Annexure IV**

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

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

4.6 On the basis of the background of the customers such as the country of origin, sources of funds, type of transactions involved, risk factors i.e. on the basis of information gathered and compiled in customer profile, indicators need to be set for such type of accounts i.e. threshold limits should be fixed for monitoring transactions in such accounts. Such threshold limits should be fixed as explained in para **3.1.5.8** above.

4.7 Periodic review of risk categorization of accounts should be done not less than once in six months and in case of need, enhanced due diligence measures should be applied **(Whenever an account/transaction is reported as suspicious to FIU-IND risk categorization in the account shall be increased by one notch meaning thereby if risk categorization of an account is low it should be changed/increased to medium, from medium to high risk and high to very high risk**

4.8 Further, the record of transactions in the accounts should be preserved / maintained in accordance with the Section 12 of the PML Act, 2002.

4.9 Branches shall also ensure that transactions of suspicious nature and / or any other type of transaction notified under Section 12 of the PML Act, 2002, are reported to the appropriate law enforcement authority.

4.10 For reporting of cash transactions aggregating Rs. 10 Lacs and above in a day, the procedure in vogue shall be followed.

4.11 Branches shall continue to maintain proper record of all cash transactions (deposits and withdrawals) of Rs. 10 lakh

and above i.e. CTRs submitted to FIU-IND placed on the NetCast Serve.

4.12 For reporting of transactions of suspicious nature, the Branches shall prepare "Suspicious Activity Report (SAR)", which shall be submitted immediately to the Principal Office through the concerned Regional Office. The SARs shall be submitted to the concerned enforcement authority immediately after ascertaining/**finalization by the principal officer (presently GM(I&C))** that the activity is actually of suspicious nature and needs reported to the authorities.

4.13 The Branch shall not reveal to either customer or any other person about the SAR, which shall be kept confidential. The Branch may enquire about the transaction or the account from the customer to get further information however, without arousing any suspicion or divulging anything. **Since tipping off is a punishable offence under PML act 2002**

4.14 Further, all new accounts shall be closely monitored for initial 6 months as per the guidelines in vogue.

4.15 Demand Drafts shall not be issued against cash for value Rs. 50000 and above and payment of fixed deposit shall not be made in cash if the amount is in excess of Rs. 20000/-

4.16 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 of the client, his business and risk profile and where necessary, the source of funds.

4.17 Multi Level Marketing Agencies

In view of the risk associated with accounts of Multi Level Marketing Agencies, while opening accounts of these marketing / trading agencies etc., branches should exercise caution & Care and follow strictly the procedure for issuance of cheque books to theses customers. **The transactions in these accounts shall be closely monitored.**

In cases where accounts have already been opened in the names of the marketing agencies, retail traders, investment firms, undertake quick reviews wherever large number of cheque books has been issued to such firms,' the relative decision may be reviewed in the light of the following: '

- Whether the cheque books have been issued to customers on the basis of their express request and after following the internal processes laid down in the matter.
- Whether the number of cheque books is consistent with/ matching the profile of the customers as also their nature of business operations.

Even where the volume of transactions/ profile of the customers apparently justify the number of cheque books issued, special ongoing monitoring of the operations in the accounts of such types of firms should be made especially if large volumes of small cash deposits are being made in those accounts and withdrawals ·are being made there from, through cheques written for small amounts, either across the counters or through clearing. In respect of such account holders banks may, in specific cases, call for the data from the account holders on the number and aggregate amount of post dated cheques issued. The data/information so collected should be analysed in select cases to rule out the possibility of the firms being engaged in deposit taking activities.

Any unusual operations noticed during the above review may be immediately reported to I&C Dept. for onward reporting/submission to other appropriate authorities such as Financial Intelligence Unit (FIU-IND). **A note in this regard is placed before Audit committee of Executives everymonth for the accounts where 25 or more than 25 cheque books were issued in a single day in a single account.**

Explanation: Cases where a large number of cheque books are sought by the company and/or multiple small deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.

5. Rejected Prospective Customers: In case of all the rejected prospective customers including those mentioned under **2.8.1 to 2.8.5**, any request letter or duly filled account opening forms, if received, record of the same shall be maintained at the branch along with the processing done and reasons of rejection given therein.

6.Risk Management

6.1 **Internal Control Systems**

Duties and responsibilities shall be explicitly allocated for ensuring that policies and procedures are managed effectively and that there is full commitment and compliance to an effective KYC Programme in respect of both existing and prospective customers. At the corporate level, Principal Officer (i.e. GM (I&C)) of senior rank shall be posted to ensure implementation and compliance and monitoring of the KYC policy and procedures along with his counterparts designated for the purpose at the **Circle Office (CO) levels**

6.2 Concurrent / Internal Audit / Inspection

Concurrent Auditor should carry out verification in respect of KYC/AML compliance in case of all accounts and transaction and submit report to the Regional Office. Regional Office should scrutinize the observation and ensure clearance, rectification by separately taking up with the branch.

Evaluation of controls for identifying high value transactions shall be carried on regular basis by the internal audit.

Concurrent/internal auditors shall specifically scrutinize and comment on the effectiveness of the measures taken by branches in implementation of the KYC Policy and procedures and steps towards prevention of money laundering. Inspection Dept., shall specifically incorporate such aspects in the Inspection Manual for the Inspectors and such compliance reports shall be placed before the Audit Committee of the Board at quarterly intervals.

6.3 Adherence to Foreign Contribution Regulation Act (FCRA), 1976

Branches shall strictly adhere to the instructions on the provisions of the Foreign Contribution Regulation Act, 1976, Master Circular regarding that giving update information is given in **Annexure VI**.

7 Product and Service Risk in view of Introduction of New Technologies - Credit Cards / Debit Cards / Smart Cards / Gift Cards

With the introduction of telephone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. The new or developing technologies including internet banking, electronic cards, that favour anonymity pose more threat from the point of view of money laundering and as such necessary measures are required to be taken to prevent use of such delivery channels in money laundering schemes.

7.1 In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, specific and adequate procedures viz. certification of all the documents presented shall also be insisted upon and, if necessary, additional documents called for, in view of the higher risk involved.

7.2 Further, first payment shall be allowed to be effected through the customer's account with another bank which adheres to KYC standards.

7.3 Marketing of these cards is generally done through the services of agents and as such appropriate KYC procedures are not only required to be applied before issuing the cards to the customers but the agents are also required to be subjected to such measures.

7.4 In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation, only such third

7.5 party shall be relied for certification / introduction, which is a regulated and supervised entity and has adequate KYC systems in place.

The Indicative list of high/medium risk products and services is given in **Appendix B**

Customer due diligence done by Intermediary: Where an intermediary is relied upon for the 'customer due diligence' (CDD) done by him, it shall be ensured that the intermediary is regulated and supervised and has adequate systems in

place to comply with the KYC requirements as the ultimate responsibility for knowing the customer lies with the bank.

8.<u>Combating of Financing of Terrorism</u> :- The United Nations periodically circulates the following two lists of individuals and entities, suspected of having terrorist links, and as approved by its Security Council (UNSC).
(a) The "ISIL (Da'esh) & Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl

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

In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time shall also be taken note of.

Banks/FIs are required to update the lists and take them into account for implementation of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, **Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated August 27, 2009.**

Before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the list. Further, branches should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to Head Office.

<u>9.Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967</u>

The procedure laid down in the UAPA Order dated March 14, 2019 (enclosed herewith as Annexure-III) shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

i) In terms of Section 51A of Unlawful Activities (Prevention) Amendment Act, 2008, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism and prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

ii) Branches are required to strictly follow the procedure laid down in the UAPA Guidelines and ensure meticulous compliance to the Order issued by the Government.

iii) On receipt of the list of individuals and entities subject to UN sanctions <u>(referred to as designated lists)</u> from RBI, bank should ensure expeditious and effective implementation of the procedure prescribed under Section 51A of UAPA in regard to freezing/unfreezing of financial assets of the designated individuals/entities enlisted in the UNSCRs and especially, in regard to <u>funds, financial assets or economic resources or related services held in the form of bank accounts</u>.

iv) In terms of Para 4 of the Order, in regard to 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 requiring them to:
a) 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 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.

b) 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 (IS.I), 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.

c) Bank shall also send by post a copy of the communication mentioned in (b) above to the UAPA nodal officer of RBI, Chief General Manager, Department of Banking Operations and Development, Central Office, Reserve Bank of India, Anti Money Laundering Division, Central Office Building, 13 th Floor, Shahid Bhagat Singh Marg, Fort, Mumbai-400 001 and also by fax at No.022-22701239. The particulars apart from being sent by post/fax should necessarily be conveyed on e-mail id: jsis@nic.in

d) Bank shall also send a copy of the communication mentioned in (b) above to the UAPA nodal officer of the State/UT where the account is held as the case may be and to FIU-India.

e) In case, the match of any of the customers with the particulars of designated individuals/entities is **beyond doubt,** the bank would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), 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.

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

v) Freezing of financial assets

a) On receipt of the particulars as mentioned in paragraph iv (b) above, IS-I 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.

b) 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 Reserve Bank of India and FIU-IND.

c) The order shall take place without prior notice to the designated individuals/entities.

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

a) 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 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.

b) 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 IS-I Division for freezing of funds or other assets.

c) The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within five working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officers in RBI. The proposed designee, as mentioned above would be treated as designated individuals/entities.

d) Upon receipt of the requests from the UAPA nodal officer of IS-I Division, the list would be forwarded to banks and the procedure as enumerated at paragraphs 2.15 [(iii), (iv) and (v)] shall be followed.

e) The freezing orders shall take place without prior notice to the designated persons involved.

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

Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the

requisite evidence, in writing, to the concerned bank. The banks 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 IS-I Division of MHA as per the contact details given in paragraph (iv)(b) above within two working days. The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) 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 fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned bank. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

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

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 RBI.

10.Geographical Jurisdictions that do not or insufficiently apply the FATF Recommendations

a) Branches are required to take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement. In addition to FATF Statements circulated by Reserve Bank of India from time to time, bank should also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. It is clarified that bank should 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. The indicative list of High/medium risk Geographies is given in Appendix C

Explanation: The process referred above does not preclude banks from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

b) Bank should 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 should, as far as possible be examined, and written findings together with all documents should be retained and made available to Reserve Bank/other relevant authorities, on request.

11.Correspondent Banking

Correspondent banking is the provision of banking services by one bank ("the correspondent bank") to another bank ("the respondent bank"). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc. Banks shall take the following precautions while entering into a correspondent banking relationship:

11.1 Sufficient information shall be gathered 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.

11.2 Correspondent Banking relationships shall be established only with the approval of the Board, or by a committee headed by the Chairman/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.

11.3 The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented.

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

11.5 The correspondent bank should ensure that the respondent bank is able to provide the relevant customer

identification
data immediately on request

11.6 Further, due caution shall be exercised while continuing relationships with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.

11.7 It shall also be ensured that the respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

12.Correspondent relationship with a "Shell Bank" Banks should 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). The correspondent bank should not permit its accounts to be used by shell banks.

13.Applicability to branches and subsidiaries outside India

The guidelines contained in this master circular shall apply to the branches and majority owned subsidiaries located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of Reserve Bank. In case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of banks are required to adopt the more stringent regulation of the two.

14.WireTransfer

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.

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

a) 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.
b) 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.
c) 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.
d) 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.

ii) 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, banks must ensure that all wire transfers are accompanied by the following information:

A) Cross-border wire transfers

i) All cross-border wire transfers **including transactions using credit or debit card** must be accompanied by accurate and meaningful
originator information.
ii) 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.

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

iii) 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 (ii) above.

(iv) All cross border wire transfers of the value of more than rupees five lakhs or its equivalent in foreign currency where either the origin or destination of fund is in India; to be reported to FIU-IND.

(B) Domestic wire transfers

i) Information accompanying all domestic wire transfers of Rs.50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.
ii) If a bank has reason to believe that a customer is intentionally structuring wire transfer to below Rs. 50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the bank must insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be made to FIU¬-IND.

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

iii) Exemptions

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

(iv) 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. The ordering bank must ensure that qualifying wire transfers contain complete originator information. The bank must 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, a bank processing an intermediary element of a chain of wire transfers must 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 must be kept at least for five years (as required under Prevention of Money Laundering Act, 2002) by 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. The beneficiary bank should 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 beneficiary bank should consider restricting or even terminating its business relationship with the ordering bank.

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

15.Maintenance of records of transactions/Information to be preserved/Maintenance and preservation of records/Cash and Suspicious transactions reporting to Financial Intelligence Unit- India (FIU-IND)

Government of India, Ministry of Finance, Department of Revenue, vide its notification dated July 1, 2005 in the Gazette of India, has notified the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the said Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts certain obligations on the banking companies in regard to preservation and reporting of customer account information. Banks are, therefore, advised to go through the provisions of PMLA, 2002 and the Rules notified there under and take all steps considered necessary to ensure compliance with the requirements of Section 12 of the Act ibid

(i) Maintenance of records of transactions

Banks should introduce a system of maintaining proper record of transactions prescribed under Rule 3 of 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 individually valued below Rupees Ten Lakh, or its equivalent in foreign currency which are that have taken place within a month and the monthly aggregate which exceeds rupees ten lakhs or its equivalent in foreign currency. It is clarified that for determining 'integrally connected transactions' 'all accounts of the same customer' should be taken into account.

c) all transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency [Ref: Government of India Notification dated November 12, 2009- Rule 3,sub-rule (1) clause (BA) of PML Rules]

d) All Cash transactions where forged or counterfeit currency notes or bank notes has been used as genuine and where any forgery of valuable security or a document has taken place facilitating the transactions and

c) All suspicious transactions, whether or not in cash made as mentioned in the Rules.

Banks/FIs are required to maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following information:

i. the nature of the transactions;
ii. the amount of the transaction and the currency in which it was denominated;
iii. the date on which the transaction was conducted; and
iv. the parties to the transaction.

(iii) Preservation/ Period of Records

I. **The Prevention of Money Laundering(Amendment Act 2012) as notified by the Government**-

In terms of Sub section 2(a) of Section 12 of the P**revention of Money laundering (Amendment) Act 2012 (**PMLA 2012) the records referred in clause (a) of Sub section (1) of Section 12 shall be maintained for a period of Five years from the date of transaction between the clients and the Banking Company.

Accordingly, banks are required to maintain for at least five years **from the date of transaction** between the bank and the client, all necessary records of transactions referred to at Rule 3 of the 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 (PMLA Rules), 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. However, records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) obtained while opening the account and during the course of business relationship, would continue to be preserved for at least Five years **after the business relationship is ended** or the account is closed whichever is later as required under Rule 10 of the Rules ibid.

Records of the identity and address of customer, and records in respect of transactions as referred to in Rule 3 be preserved in hard or soft format so that same is retrieved easily and quickly whenever required or when requested by the competent authorities.

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

v) Reporting to Financial Intelligence Unit – India

a) In terms of the PMLA rules, banks are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 **Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof**. at the following address:

Director,FIU-IND,
FinancialIntelligenceUnit-India,
6thFloor,HotelSamrat,
Chanakyapuri,
NewDelhi-110021.
Website - http://fiuindia.gov.in/

Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the REs for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

b) Banks should carefully go through all the reporting formats. There are altogether eight reporting formats, viz. i) Cash Transactions Report (CTR); ii) Summary of CTR iii) Electronic File Structure-CTR; iv) Suspicious Transactions Report (STR); v) Electronic File Structure-STR; vi) Counterfeit Currency Report (CCR); vii) Summary of CCR and viii) Electronic File Structure-CCR. The reporting formats contain detailed guidelines on the compilation and manner/procedure of submission of the reports to FIU-IND. It would be necessary for banks to initiate urgent steps to ensure electronic filing of all types of reports to FIU-IND. The related hardware and technical requirement for preparing reports in an electronic format, the related data files and data structures thereof are furnished in the instructions part of the concerned formats.

c) FIU-IND have placed on their website editable electronic utilities to enable banks to file electronic CTR/STR who are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data base. It is, therefore, advised that in cases of banks, where all the branches are not fully computerized, the Principal Officer of the bank should cull out the transaction details from branches which are not yet computerized and suitably arrange to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND in their website http://fiuindia.gov.in.

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

fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.

d) Banks are required to prepare a profile for each customer based on risk categorization. Further, periodical review of risk categorization has been emphasized. It is, therefore, reiterated that, as a part of transaction monitoring mechanism, an appropriate software application is required to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers. It is needless to add that a robust software throwing alerts is essential for effective identification and reporting of suspicious transaction

The Bank has purchased an AML software from IDBI Intech a subsidiary of IDBI Bank ltd.The CTR/STR are generated through the software automatically and are reported to FIU-IND at their website

16.Cash and Suspicious Transaction Reports

a) Cash Transaction Reports (CTRs)

While detailed instructions for filing all types of reports are given in the instructions part of the related formats, bank should scrupulously adhere to the following:

i) The Cash Transaction Report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month. Cash transaction reporting by branches to their controlling offices should, therefore, invariably be submitted on monthly basis **(not on fortnightly basis)** and banks should 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 should be reported by the Principal Officer of the bank to FIU-IND in the specified format(Counterfeit Currency Report – CCR), by 15thday of the next month. These cash transactions should 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 should 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 should be compiled by the Principal Officer of the bank every month in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted to FIU-India.
vi) 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 :

a) The CTR is to be generated in the format prescribed by FIU-IND;

b) A copy of the monthly CTR submitted on its behalf to FIU-India is available at the concerned branch for production to auditors/inspectors, when asked for; and

c) The instruction on 'Maintenance of records of transactions; 'Information to be preserved' and 'Maintenance and Preservation of records' are scrupulously followed by the branch.

b) Suspicious Transaction Reports (STRs)

i) While determining suspicious transactions, bank should be guided by definition of suspicious transaction 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. It is clarified that bank should report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction **as offline STR.**
iii) Bank should make STRs if has reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of ScheduleofPMLA,2002 .
iv) The Suspicious Transaction Report (STR) should 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 should record his reasons for treating any transaction or a series of transactions as suspicious. It should 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 should 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, bank may consider the indicative list of suspicious activities contained in Annex-E of the 'IBA's Guidance Note for Banks, 2009'.

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

c) Non-Profit Organization: (NTR)

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

d) Cross border wire transfer (CBWT) - CBWT is required to be filed by 15th of succeeding month for all cross border wire transfers of the value more than Rs. five lakh or its equivalent in foreign currency where either the origin or destination of funds is in India.

e) Counterfeit Currency report - CCR is required to be filled by 15th of succeeding month for all counterfeit notes detected by the branches during the month.

17.Guidance against "Tipping Off"

Senior Management should provide sufficient guidance to staff to ensure that the customers are not informed (i.e. tipped off) that his/her accounts are under monitoring for suspicious activities and/or that a disclosure has been made to FIU-IND.

The Bank can however make normal enquiries to learn more about the transaction or instruction to determine whether the activities of the customer arouse suspicion.

Where it is known or suspected that a STR has already been made internally or externally, and it then becomes necessary to make further enquiries, care must be taken to ensure that the suspicion is not disclosed either to the client or to any other third party. Subject to internal procedures, such enquiries should normally/only be made as directed by the Principal Officer (PO).

PMLA mandates that the STR related information should not revealed to the customers to avoid prejudicing or affecting an investigation, which may be initiated by the law enforcement agencies.

Thus, it is essential that all of the aforesaid activities of reporting of the confirmed matches are kept strictly confidential.

Records of all such reports and investigations should be kept securely and separately so as not to mix with general transactional data. Custody of such records may be entrusted with staff of sufficient seniority or responsibility.

Customers should not be informed of any such reports in any circumstances to avoid "TIPPING OFF" offence.

18. **KYC for the Existing Accounts**

18.1 While the Revised Guidelines as above will apply to all new customers, the same shall apply on existing accounts on the basis of materiality and risk i.e. those accounts perceived to be of high or very high risk.

18.2 Branches shall also ensure that all existing accounts of companies, firms, trusts, charities, religious organizations and other institutions are subjected to minimum KYC standards which would establish the identity

of the natural / legal person and those of the 'beneficial owners'. In this regard, Branches were earlier advised to certify compliance of the KYC Norms in case of all existing accounts by 31.12.04.

18.3 Transactions shall however be monitored continuously in the existing accounts and any unusual pattern in the operation of the account shall trigger a review of the customer due diligence measures i.e. the KYC procedures shall have to be applied to such accounts. Monetary limit for monitoring of transactions in these accounts shall also be in line with the guidelines in vogue.

18.4 Further, term / recurring deposit accounts or accounts of similar nature shall be treated as new accounts at the time of renewal and subjected to revised KYC procedures.

18.5 Where the branch is unable to apply appropriate KYC measures due to non-furnishing of information and / or non-cooperation by the customer, the branch after making all efforts may consider closing the account or terminating the banking / business relationship. However, guidelines / procedure in this regard i.e. for terminating customer relationship shall be followed as given in **2.7** above.

19. Role of AML Cell / Dept. at Head Office

In view of the dimension and the implications of KYC / AML and its dynamic nature, it becomes necessary to have a separate / dedicated Cell / Dept. at the Head Office level. The Cell / Dept., preferably with independent setup, should be adequately and appropriately staffed with all proficient in working on computers / in computerized environment and able to use IT / software solutions.

The Cell / Dept. should be headed by an executive in the rank of an Asst. General Manager / **Chief Manager under overall supervision** of GM (I&C) who is designated as the Principal Officer of the Bank.

Further reporting of any violation under AML shall be reported to designate authority by Principal officer (presently GM(I&C).

The role of the AML Cell / Dept. is,

1. Provide necessary guidance / decisions on KYC (Vertical-CS&P) and AML related issues to branches, user offices / departments of the bank;

2. Implement and monitor compliance of the policy guidelines, in this regard;

3. Analyze, evaluate risks associated with different customer segments, activities etc., advise branches / offices and contribute in future planning process, accordingly;

4. Arrive at the threshold limits, customer segment-wise / customer-activity wise etc and as directed by the Govt. / Reserve Bank of India for monitoring of transactions in accounts.

5. Ensure entire staff gets training / exposure on these issues with front desk, back desk, managerial and control specific approach and devise means and mechanism for customer education;

6. Analyze 'Suspicious Activity Reports (SARs)' as may be received from the branches / offices, investigate and cull the false ones and report the actual ones to the designated authorities viz. Director as given in The Prevention of Money Laundering Act, 2002 or as may be specified by the Govt. of India / Reserve Bank of India;

7. Deal with all money-laundering cases in co-ordination with other concerned Head Office Depts., particularly Vigilance, I&C and Personnel;

8. Devise system and mechanism for ensuring submission and reporting of all the necessary reports by the branches / offices of the bank to the designated authorities;

9. Liaison with the related / enforcement agencies / offices of Govt. / RBI etc.

10. Liaison with the outside, domestic as well as international, agencies for updating information on prohibited / banned individuals and entities;

11. Explore and make arrangements with different organizations / agencies for accessing their databases, that help in establishing identities of individuals and entities;

12. Provide / help in acquiring software solution for monitoring of transactions in customer accounts, generation of reports and for customer profiles;

13. Get KYC (Vertical-IBD) / AML Status Reports of Correspondents / Respondents / Banks / Financial Institutions, with whom bank may enter into some business relationship;

14. Keep abreast with the related Laws / Rules / Regulations / KYC (Vertical-CS&P) and AML related developments;

15. Collect all necessary data / information / reports from the branches either directly or through concerned **Circle**

Offices (Cos) / Offices of the bank; and

16. Report / Submit all necessary information / reports / notes / reviews before the Top Management / Board of Directors and Audit Committee of the Board.

Principal Officer and his Role

As already submitted, the AML Cell / Dept. should be headed by a senior management official in the rank of an Asst. General Manager/Chief Manage under Overall supervision of General Manager (I&C), who is designated as the Principal Officer of the Bank. The official posted as the Head of the AML Cell / Dept. should be able to assist the Principal Officer in carrying his below mentioned role smoothly. To ensure this he should,

- have sufficient operational experience and investigative mind, and able to act freely,
- be responsible for monitoring and reporting of all the transactions and sharing of information as required under the law and as per policy guidelines of the bank,
- 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.
- prepared necessary reports for placing before the Top Management viz. Executive Director or Chairman & Managing Director or Board of Directors
- enable Principal Officer of the Bank to carry his role as given under:

Principal Officer has a key role to play in ensuring compliance with the Anti Money Laundering guidelines without compromising on business interests of the bank. In discharge of his function he will have to maintain communication links with the Regulator (RBI, SEBI, Govt. etc), Branches and **Circle Offices**, Investigating Agencies, Personnel Department/ HRD / Staff Training Colleges / Other concerned Head Office Departments viz. IBD, MBD, Credit, SLPS, I&C, Vigilance etc., Other relevant Organizations / Banks (National as well as International).

i) To establish and implement policies, procedures and controls, which aim to deter criminal elements from using products and services for money- laundering.

ii) To activate KYC (**Vertical-Operations**) / Customer Identification Procedures so as to identify the users/customers, Principal beneficial owners (Vertical-Compliance), Origin of funds, Nature of business, Transactions those are abnormal within the relationship etc.

iii) To lay down clear reporting lines and procedure for suspicious transactions and ensure that all such reports reach him without delay.

iv) To ensure that relevant records are maintained for an effective retention period as may be determined at the end of a business relationship in line with the various legal and directed requirements, if any, but not less than **5** years in any case.

v) To keep himself abreast of the latest developments in AML area in other organizations/countries and report to top management, accordingly.

vi) To maintain among other things, the

- List of high risk countries; (Vertical-IBD)
- Identify high, medium and low risk activities; (Vertical-CS&P)
- Identify and define unusual or suspicious transactions;
- Put in place procedure for regular periodical updating of customer profiles. (Vertical-CS&P)

vii) To initiate follow up action on unusual or suspicious activity and co-ordinate with branch / concerned regional office functionaries in deciding on the desirability of continuing the account with increased caution and monitoring or to close the account.

viii) To decide on whether to report the relationship to regulatory or law enforcement authorities. This shall be purely from the point of view of KYC or AML purposes.

ix) To prepare adequate training material for the operating staff and take such steps as are necessary to ensure that

arrangements are made to train concerned staff. In effect there has to be an attitudinal change in the outlook of the operating staff that should be on guard at all times.

x) To arrange for the creation of a suitable database, information system, which can be drawn upon in case of need and to share information with regulators, other banks, institution, etc.

xi) To take proactive measures to analyze suspicious activities reported and track pattern, which could be brought to the notice of the operating staff to enable the staff to remain vigilant against similar transactions.

xii) To put in place a reporting system through which to periodically report to the Top Management / Board of Directors and to conduct an annual review of anti-money laundering activities in the Bank, etc.

At the CO level, for effective implementation and compliance of the policy guidelines on KYC and AML, while the **CO** shall himself oversee the implementation and compliance of the Guidelines, a senior official in the rank of either AGM or CM shall be designated as **Circle/CLUSTER** Principal Officer **(CPO),** to follow up with the Branches / Offices and to liaison with the Head of the AML Cell / Dept. and Principal Officer at Head Office.

Designated Director and his role

As per the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Rules), to ensure overall compliance with the obligations under the Act and Rules, Executive Director has been nominated as "Designated Director" and has been communicated to the Director, Financial Intelligence Unit-India(FIU-IND)

20.IT Solution

In order to effectively implement and monitor the KYC Policy, it is necessary to have software solution particularly for monitoring transactions in accounts, evaluating risk, working with threshold limits and for report generation. The software will generate alerts on different scenarios and risk factors to detect potentially suspicious activities.

21.Customer Education & Staff Training

Implementation of KYC procedures requires specific information to be collected from the customers, which some customers may consider of personal nature or which were hitherto never called for from him by the bank or any other earlier or present bank. This may sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. There is, therefore, a need for educating customers about the objectives of the KYC programme and AML issues and the legal and other obligations that banks have to accomplish. This besides creating necessary awareness amongst the customers requires exposing / training staff, particularly those at the front and back desks, at the branches as well, who need to be more conversant with these issues and able to handle such situations amicably while dealing with the customers.

21.1 Necessary ongoing Training Programmes shall be conducted on KYC /AML/CFT with front line, back desk, managerial and control specific approach so that persons be adequately trained and well-versed in KYC/AML/CFT policies

21.2 Besides, for creating necessary awareness amongst the customers, specific literature, brochures / pamphlets and posters shall be prepared for display and distribution.

21.3 Adequate screening mechanism be applied during personnel recruitment/hiring process.

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

Under FATCA and CRS, REs shall adhere to the provisions of Income Tax Rules 114F, 114G and 114H and determine whether they are a Reporting Financial Institution as defined in Income Tax Rule 114F and if so, shall take following steps for complying with the reporting requirements:

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

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

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

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

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

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

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

a) updated Guidance Note on FATCA and CRS b) a press release on 'Closure of Financial Accounts' under Rule 114H (8).

Annexure- I (OBC KYC/AML FY-2019-20 & onwards)

Customer Identification Procedure
Documents that may be obtained from customers

	Proposed
Customers/Clients	**Documents as per CDD Measures** (Certified copy of each of the following document shall be obtained)
1. Accounts of individuals - Proof of Identity and Address	**Customer Due Diligence (CDD) Procedure in case of Individuals:-** For undertaking CDD, the following shall be obtained from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity: (a) a certified copy of any *OVD containing details of his identity and address (b) one recent photograph (c) the Permanent Account Number or Form No. 60 as defined in Income-tax Rules, 1962, and (d) such other documents pertaining to the nature of his/her business or financial status. Provided that, i) Aadhaar number from an individual, who is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016), shall be obtained. On receipt of the Aadhaar number from the customer, authentication of the customer's Aadhaar number may be carried out using e-KYC authentication facility provided by the Unique Identification Authority of India upon receipt of the customer's declaration that he/ she is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 (18 of 2016) in his/ her account. ii) Aadhaar authentication/ offline-verification may be carried out in case of an individual who voluntarily uses his Aadhaar number for identification purpose. In cases where successful authentication has been carried out, other OVD and photograph need not be submitted by the customer. Provided further that in case biometric e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar

	causes, Bank shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD from the customer. CDD done in this manner shall invariably be carried out by an official of the Bank and such exception handling shall also be a part of the concurrent audit. Bank shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Bank and shall be available for supervisory review. Explanation 1: Bank shall, where its customer submits his Aadhaar number, ensure such customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act. Explanation 2: Biometric based e-KYC authentication can be done by bank official/ business correspondents/ business facilitators. ***Officially Valid Document (OVD)** means the passport, the driving licence, **proof of possession of Aadhaar number**, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and **letter issued by the National Population Register containing details of name and address.** Provided that, a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India. b. where the OVD furnished by the customer does not have updated address, the following documents shall be **deemed to be OVDs for the limited purpose of proof of address**:- i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); ii. property or Municipal tax receipt; iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; iv. letter of allotment of accommodation from employer issued by State

	Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation; c. the customer shall submit OVD with current address within a period of **three** months of submitting the documents specified at 'b' above d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address. Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.
2. Accounts of Companies	(a) Certificate of incorporation; (b) Memorandum and Articles of Association; (C) Prior to opening of account, the data of Shell Companies at ROC be verified; (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) Documents as specified in Customer Due Diligence (CDD) Procedure applicable for individuals, in respect of managers, officers or employees holding an attorney to transact on its behalf;** and **(f) Permanent Account Number (PAN) of the company** **<u>One Person Company</u>**-The KYC documents required for private limited company constituted under OPC will remain same as are for other private limited companies except that in case of OPC, KYC documents of nominee as per memorandum of company be also obtained by branch
3. Accounts of Partnership firms	a) registration certificate; (b) partnership deed; **(c) Permanent Account Number (PAN) of the partnership firm; and** (d) **Documents as specified in Customer Due Diligence (CDD) Procedure applicable for individuals, in respect of the person holding an attorney to transact on its behalf.**
4. Accounts of Trusts	(a) registration certificate; (b) trust deed; (c) **Permanent Account Number (PAN) or Form No.60 of the Trust; and** (d) **Documents as specified in Customer Due Diligence (CDD) Procedure applicable for individuals, in respect of the person holding a power of attorney to transact on its behalf.**
5. Accounts of unincorporated association or a body of individuals (including unregistered Partnership Firms / Trusts)	**(a)** Resolution of the managing body of such association or body of individuals; (b) **Permanent Account Number (PAN) or Form No.60 of the unincorporated association or a body of individuals**; **(c)** Power of attorney granted to him to transact on its behalf;

	(d) Documents as specified in Customer Due Diligence (CDD) Procedure applicable for individuals, in respect of the person holding an attorney to transact on its behalf. **(e)** Such information as may be required by the Bank to collectively establish the legal existence of such an association or body of Individual's. (the documents like Certificate/registration document issued by professional tax authorities, License issued by the Registering authority like certificate of Practice issued by Indian Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, etc., the complete Income Tax return (*not just the acknowledgement*) etc.) as applicable **(f)** In case of unregistered Partnership/ Trust, Partnership Deed / Trust Deed shall be obtained in addition to above documents
6. Juridical persons, such as societies, universities and local bodies like village panchayats	i. Document showing name of the person authorised to act on behalf of the entity; ii. **Documents as specified in Customer Due Diligence (CDD) Procedure applicable for individuals, in respect of the person holding an attorney to transact on its behalf.** and iii. Such documents as may be required by the Bank to establish the legal existence of such an entity/ juridical person.
7. Accounts of Proprietorship Concerns	a. Registration certificate (in the case of a registered concern) b. Certificate/license issued by the Municipal authorities under Shop & 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. License issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, etc. g. Registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority / Department. h. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of bank account. i. The complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected duly authenticated/acknowledged by the income Tax Authorities. j. Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern. Any two of the above documents would suffice. These documents should be in the name of the proprietary concern. .In case two documents not available then for one document Contact point verification can be undertaken. In addition to the above, **Customer Due Diligence (CDD) Procedure applicable for individual (proprietor) shall be carried out.**
Supporting Document for TIN (For FATCA/CRS)	Copy of any of these - T- TIN, C- Company Identification Number, G- US GIIN, E- Global Entity Identification Number (EIN), O- Other

Annexure 1(a)

LIST OF KYC DOCUMENTS FOR **NON-RESIDENT** ACCOUNT OPENING

Description	Non Resident Indian	OCI / PIO	Non-Resident (Foreign- Nationals /Student)	NRIs with Seafarer work profile
Identity Document (Any one of the following)	Copy of Relevant Pages of Passport	Copy of Relevant Pages of Passport	Copy of Relevant Pages of Passport	Copy of Relevant Pages of Passport
Local Address Proof (Any one of the following)	Valid Indian Passport, Voter ID card(election card), Valid Indian driving license, Job Card issued by NREGA duly signed by an officer of the State Government, Letter / proof of possession of Aadhaar number Provided that he may submit it in such form as are issued by the Unique Identification Authority of India.	Relevant pages of Passport (mentioning overseas address), Self-declaration of address with positive confirmation.	Self Declaration with validity 30 Days and after that local address proof need to be submitted such as employer certificate, ID Card (having address) notarized copy of Rental Agreement, Telephone Bill, Electricity Bill etc	Valid Indian Passport, Voter ID card(election card), Valid Indian driving license, Job Card issued by NREGA duly signed by an officer of the State Government, Letter / proof of possession of Aadhaar number Provided that he may submit it in such form as are issued by the Unique Identification Authority of India.
Overseas Address Proof (Any one of the following)	Relevant pages of Passport (mentioning overseas address), Self-declaration of address with positive confirmation by submitting a copy of anyone of the following- Government issued National Identity Card at the country of residence, Driving License issued abroad, Utility Bill (Electricity, Telephone, Gas),Original copy of latest overseas bank account or existing NRE / NRO account statement carrying overseas address, Employer's certificate, Address proof of the blood relative as per point a) to e) above	Relevant pages of Passport (mentioning overseas address), Self-declaration of address with positive confirmation by submitting a copy of anyone of the following- Government issued National Identity Card at the country of residence, Driving License issued abroad, Utility Bill (Electricity, Telephone, Gas),Original copy of latest overseas bank account or existing NRE / NRO account statement	Relevant pages of Passport (mentioning overseas address), Government issued National Identity Card of the country of residence, Driving License issued abroad, Original copy of latest overseas bank account or existing NRE / NRO account statement carrying overseas address, Employer's certificate, Institute Certificate or any Certificate issued by local Indian authority confirming Overseas Address.	NRIs with seafarer work profile and on ship, can either give Employer's overseas address or Indian address.

	(spouse, father, mother, sister, brother and child) with whom you are staying along with supporting proof of relationship (Passport, PAN Card, Driving License, Voter Identity Card, Aadhaar Card, Marriage Certificate, Birth Certificate)	carrying overseas address, Employer's certificate, Address proof of the blood relative as per point a) to e) above (spouse, father, mother, sister, brother and child) with whom you are staying along with supporting proof of relationship (Passport, PAN Card, Driving License, Marriage Certificate, Birth Certificate)		
Status Proof	Valid Visa, Work Permit, Job Contract, Resident Card or equivalent proof which ascertain NRI status.	PIO/OCI Card, Copy of Marriage Certificate, Certificate issued by Indian Embassy proving customer PIO status, Grandparents passport, establishing Indian Origin	Copy of Relevant Pages of Passport	Valid Job Contract, Continuous Discharge Certificate (CDC), if the disembarkation stamp on CDC is not more than 6 months old, Expired contract letter (if the disembarkation stamp on CDC is not more than 6 months old),Last pay slip evidencing employment with a shipping company (not more than 6 months old)
Additional Document	II) FATCA Declaration with functional Equivalent Document. III) PAN /Form 60.	II) FATCA Declaration with functional Equivalent Document. III) PAN /Form 60.	II) FATCA Declaration with functional Equivalent Document. III) PAN/Form 60.	II) FATCA Declaration with functional Equivalent Document. III) PAN/Form 60.
**** In the case of persons who are leaving India for taking up employment abroad/education Purpose, NRE/NRO accounts can be opened but will have to be activated only after their departure from India. [i.e. only after the prospect becomes non-resident and not before].***				
*****In Case of Non face to face customers the customer may send the duly filled up AOF along with relevant KYC Documents* certified by any one of the following:** **• Authorized officials of overseas branches of Scheduled Commercial Banks registered in India,** **• branches of overseas banks with whom Indian banks have relationships,** **• Notary Public abroad,**				

• Court Magistrate, **• Judge,** **• Indian Embassy/Consulate General in the country where the non-resident customer resides.**
****** In case of KYC Documents in foreign language other than English , Customer has to submit translated copy (duly Attested)***

Annexure II (OBC KYC/AML-FY 2019-20)

Basel Committee on Banking Supervision

"Customer due diligence for banks"

Excerpts from the paper on 'Customer due diligence for banks'

- Importance of KYC Standards for Supervisors and Banks -

'Sound KYC procedures have particular relevance to the safety and soundness of banks, in that:

- they help to protect banks' reputation and the integrity of banking systems by reducing the likelihood of banks becoming a vehicle for or a victim of financial crime and suffering consequential reputational damage;
- they constitute an essential part of sound risk management (e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management).

The inadequacy or absence of KYC standards can subject banks to serious customer and counterparty risks, especially ***Reputational, Operational, Legal and Concentration Risks***. All these risks are interrelated. However, any one of them can result in significant financial cost to banks (e.g. through the withdrawal of funds by depositors, the termination of inter-bank facilities, claims against the bank, investigation costs, asset seizures and freezes, and loan losses), as well as the need to divert considerable management time and energy to resolving problems that arise.

Reputational risk poses a major threat to banks, since the nature of their business requires maintaining the confidence of depositors, creditors and the general marketplace. Reputational risk is defined as the potential that adverse publicity regarding a bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Banks are especially vulnerable to reputational risk because they can so easily become a vehicle for or a victim of illegal activities perpetrated by their customers. They need to protect themselves by means of continuous vigilance through an effective KYC programme. Assets under management, or held on a fiduciary basis, can pose particular reputational dangers.

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. Most operational risk in the KYC context relates to weaknesses in the implementation of banks' programmes,

ineffective control procedures and failure to practise due diligence. A public perception that a bank is not able to manage its operational risk effectively can disrupt or adversely affect its business.

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 a bank. Banks may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practice due diligence. Consequently, banks can, for example, suffer fines, criminal liabilities and special penalties imposed by supervisors. Indeed, a court case involving a bank may have far greater cost implications for its business than just the legal costs. Banks will be unable to protect themselves effectively from such legal risks if they do not engage in due diligence in identifying their customers and understanding their business.

Supervisory concern about ***concentration risk*** mostly applies on the assets side of the balance sheet. As a common practice, supervisors not only require banks to have information systems to identify credit concentrations but most also set prudential limits to restrict banks' exposures to single borrowers or groups of related borrowers. Without knowing precisely who the customers are, and their relationship with other customers, it will not be possible for a bank to measure its concentration risk. This is particularly relevant in the context of related counterparties and connected lending.

On the liabilities side, concentration risk is 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. Funding risk is more likely to be higher in the case of small banks and those that are less active in the wholesale markets than large banks. Analyzing deposit concentrations requires banks to understand the characteristics of their depositors, including not only their identities but also the extent to which their actions may be linked with those of other depositors. It is essential that liabilities managers in small banks not only know but maintain a close relationship with large depositors, or they will run the risk of losing their funds at critical times.

Customers frequently have multiple accounts with the same bank, but in offices located in different countries. To effectively manage the reputational, compliance and legal risk arising from such accounts, banks should be able to aggregate and monitor significant balances and activity in these accounts on a fully consolidated worldwide basis, regardless of whether the accounts are held on balance sheet, off balance sheet, as assets under management, or on a fiduciary basis.'

****

Annexure III (OBC KYC/AML FY-2019-20)

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

New Delhi, dated 14 March 2019

ORDER

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

The Unlawful Activities (Prevention) Act, 1967 (UAPA) was amended and notified on 31.12.2008, which, inter-alia, inserted Section 51A to the Act. Section 51 A, reads as under:-

"51A. For the prevention of, and for coping with terrorist activities, the Central Government shall have power to —
(a) freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;

(b) prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism:

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

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

"Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order. 2007, as may be amended from time to time.
In order to expeditiously and effectively implement the provisions of Section 51A, a procedure was outlined vide this Ministry Order No. 17015/10/2002-IS-VI dated 27.08.2009. After the reorganization of the Divisions in Ministry of Home Affairs, the administration of Unlawful Activities (Prevention) Act, 1967 and the work relating to countering of terror financing has been allocated to the CTCR Division. The order dated 27.8.2009 is accordingly modified as under:
Appointment and communication of details of UAPA Nodal Officers
2. As regards appointment and communication of details of UAPA Nodal Officers-

(i) The UAPA Nodal Officer for CTCR Division would be the Joint Secretary (CTCR), Ministry of Home Affairs. His contact details are 011-23092736 (Tel), 011-23092569 (Fax) and jsctcr-mha@gov.in (e-mail id).
(ii) The Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, FIU-IND; and RBI, SEBI, IRDA (hereinafter referred to as Regulators) shall appoint a UAPA Nodal Officer and communicate the name and contact details to the CTCR Division in MHA.
(iii) The States and UTs should appoint a UAPA Nodal Officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the CTCR Division in MHA.

(iv) The CTCR Division in MHA would maintain the consolidated list of all UAPA Nodal Officers and forward the list to all other UAPA Nodal Officers.
(v) The RBI, SEBI, IRDA should forward the consolidated list of UAPA Nodal Officers. to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively.
(vi) The consolidated list of the UAPA Noda! Officers should be circulated by the Nodal Officer of CTCR Division of MHA in July every year and on every change. Joint Secretary (CTCR) being the Nodal Officer of CTCR Division of MHA, shall cause the amended list of UAPA Noda! Officers to be circulated to the Nodal Officers of Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, RBI, SEBI, IRDA and FIU-IND.

Communication of the list of designated individuals/entities

3. As regards communication of the list of designated individuals/entities-
(i) The Ministry of External Affairs shall update the list of individuals and entities subject to UN sanction measures on a regular basis. On any revision, the Ministry of External Affairs would electronically forward this list to the Nodal Officers in Regulators, FIU-IND, CTCR Division and Foreigners Division in MHA,
(ii) The Regulators would forward the list mentioned in (i) above (referred to as designated lists) to the banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies respectively.
(iii) The CTCR Division of MHA would forward the designated lists to the UAPA Nodal Officer of all States and UTs.
(iv) The Foreigners Division of MHA would forward the designated lists to the immigration authorities and security agencies.

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

4. As regards funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc., the Regulators would forward the designated lists to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively. The RBI, SEBI and IRDA would issue necessary guidelines to banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies 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 Order, herein after, referred to as designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or Insurance policies etc., with them.
(ii) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies 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, stocks or Insurance policies etc., 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 or 011-23092736. The particulars apart from being sent by post, should necessarily be conveyed on e-mail id: jsctcr-mha@gov.in.
(iii) The banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall also send a copy of the communication mentioned in (ii) above to the UAPA Nodal Officer of the State/UT where the account is held and Regulators and FIU-IND, as the case maybe.

(iv) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies would prevent designated persons from conducting financial transactions, under intimation 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 id: jsctcr-mha@gov.in.
(v) The banks, stock exchanges /depositories, intermediaries regulated by SEBI and insurance companies, shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (ii) above, carried through or attempted as per the prescribed format.

5. On receipt of the particulars referred to in paragraph 4(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, stock exchanges/depositories, intermediaries regulated by SEBI and Insurance Companies are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies are held by the designated individuals/entities This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.
6. In case, the results of the verification indicate that the properties are owned by or are held for the benefit of the designated individuals/entities, an order to freeze these assets under Section 51A of the UAPA would be issued by the UAPA Nodal Officer of CTCR Division of MHA and conveyed electronically/to the concerned bank branch, depository, branch of insurance company 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 ail 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 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 to all Directors General of Police/ Commissioners of Police of all States/UTs for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967.

The order shall be issued without prior notice to the designated individual/entity.
Regarding financial assets or economic resources of the nature of immovable properties

7. CTCR Division of MHA would electronically forward the designated lists to the UAPA Nodal Officer of all States and 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.

8. 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 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 would necessarily be conveyed on e-mail id jsctcr-mha@gov.in.

9. 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 id given below. 10. A copy of this reference should be sent to Joint Secretary (CTCR), Ministry of Home Affairs, at Fax No.011-23092569 and also conveyed over telephone on 01123092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail id: jsctcr-mha@gov.in. MHA may also have the verification conducted by the Central Agencies. This verification would be completed within a maximum of 5 working days.
11. 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, by the UAPA 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 be issued without prior notice to the designated individual/entity.
12. 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 1967.

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

13. 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.

14. 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.

15. 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.

16. Upon receipt of the requests by these Nodal Officers from the UAPA nodal officer of CTCR Division, the procedure as enumerated at paragraphs 4 to 12 above shall be followed.

The freezing orders shall be issued 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

17. Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence. in writing, to the concerned bank, stock exchanges/ depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State/UT Nodal Officers.

18. The banks, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, 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 4 (ii) above, within two working days.

19. The Joint Secretary (CTCR), MHA being the UAPA 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 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 15 working days, the UAPA Nodal Officer of CTCR Division shall inform the applicant.

Communication of Orders under section 51A of Unlawful Activities (Prevention) Act, 1967.

20. All Orders under section 51A of Unlawful Activities (Prevention) Act, 1967 relating to funds, financial assets or economic resources or related services, would be communicated to all the banks, depositories/stock exchanges, intermediaries regulated by SEBI, insurance companies through respective Regulators, and to all 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

21. 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.

22. 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 51A

23. 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.

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

(Piyush Goyal)
Joint Secretary to the Government of India

ANNEXURE IV (OBC KYC/AMLFY-2019-20)

Indicative Alert indicators for branches/Departments

	Alert Indicator		**Indicative Rule / Scenario**
1	CV1.1	Customer abandoned the transaction for the KYC requirement.	Customer left without completing the transaction after being informed about KYC requirements.
2	CV2.1	Customer offered false or forged identification documents	Customer gives false identification documents or documents that appears to be counterfeited, altered or inaccurate
3	CV3.1	Address non-existent at the time of account opening	Address provided by the customer is found to be nonexistent. If letter of thanks sent to customer returns due to address nonexistent, branch should ensure that the address provided by the customer is nonexistent by making personal visit to the address provided, may be reported as Off-line alert.
4	CV3.2	Address found to be wrong at the time of account opening	Customer not staying at address provided during account opening
5	CV4.1	Complex structure created to avoid identification of beneficial owner	Customer uses complex legal structures or where it is difficult to identify the beneficial owner
6	LQ2.1	Customer being investigated for select criminal offences	Customer has been the subject of inquiry from any law enforcement agency relating to TF or terrorist activities
7	MR1.1	Adverse media report for criminal activities	Match of customer details with persons reported in local media / open source for criminal offences
8	MR2.1	Adverse media report about terrorist activities of customer	Match of customer details with persons reported in local media / open source for terrorism or terrorist financing related activities
9	EI 1.1	Customer abandoned the transaction when questioned	Customer did not complete transaction after queries such source of funds etc.
10	EI 2.1	Customer body language based alert	Customer's body language shows he is in hurry or nervous
11	EI 2.3	Customer provides inconsistent information	Customer changes the information provided after more detailed information is requested

			Customer provides information that seems minimal, possibly false or inconsistent
12	EI 3.1	Customer appears to be acting on behalf while posing in-person	Customer has vague knowledge about amount of money involved in the transaction Customer taking instructions for conducting transactions Customer is accompanied by unrelated individuals.
13	EI 4.1	Customer avoiding nearer branches without rationale	Customer travels unexplained distances to conduct transactions
14	EI 4.2	Customer offers different identifications on different occasions	Customer offers different identifications on different occasions with an apparent attempt to avoid linkage of multiple transactions
15	EI 4.3	Customer purposely wants to avoid reporting	Customer makes inquiries or tries to convince staff to avoid reporting
16	EI 4.4	Customer is not able to explain the source of funds	Customer could not explain source of funds satisfactorily
17	EI 5.1	Transaction is unnecessarily made to be complex	Transaction is unnecessarily complex for its stated purpose
18	EI 5.2	Transaction has no economic rationale	The amounts or frequency or the stated reason of the transaction does not make sense for the particular customer
19	EI 5.3	Transaction inconsistent with business/ profile	Transaction involving movement of which is inconsistent with the customer's business
20	PC1.1	Complaint received from public	Complaint received from public for abuse of account for committing fraud etc.
21	BA1.1	Alert raised by agent	Alert raised by agents about suspicion
22	BA1.2	Alert raised by other institution	Alert raised by other institutions, subsidiaries or business associates including cross-border referral
23	TY3.1	Customer trying to avoid linkage	customer providing different IDs or date of birth at different instances.

Annexure - V (OBC KYC/AMLFY-2019-20)

Government of India
Ministry of Finance
(Department of Revenue)
Notification

New Delhi, the 16th December 2010

GSR ------ (E) – In exercise of the powers conferred by sub-section (1) read with clauses (h) (i), (j) and (k) of sub-section (2) of Section 73 of the Prevention of Money-laundering Act, 2002 (15 of 2003), the Central Government hereby makes the following amendments to the 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, namely::-

1. (1) These rules may be called the 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) Third Amendment Rules, 2010.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. In the 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, -

(a) in rule 2,-

(i) after clause (b), the following clause shall be inserted, namely:-

"(bb) "Designated Officer" means any officer or a class of officers authorized by a banking company, either by name or by designation, for the purpose of opening small accounts".

(ii) in clause (d), for the words "the Election Commission of India or any other document as may be required by the banking company or financial institution or intermediary", the words "Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, the letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number or any other document as notified by the Central Government in consultation with the Reserve Bank of India or any other document as may be required by the banking companies, or financial institution or intermediary" shall be substituted;

(iii) after clause (fa), the following clause shall be inserted, namely:-

"(fb) "small account" means a savings account in a banking company where-

(i) the aggregate of all credits in a financial year does not exceed rupees one lakh,

(ii) the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand, and;

(iii) the balance at any point of time does not exceed rupees fifty thousand".

(b) In rule 9, after sub-rule (2), the following sub-rule shall be inserted, namely:-

"(2A) Notwithstanding anything contained in sub-rule (2), an individual who desires to open a small account in a banking company may be allowed to open such an account on production of a self-attested photograph and affixation of signature or thumb print, as the case may be, on the form for opening the account.

Provided that –

(i) the designated officer of the banking company, while opening the small account, certifies under his signature that the person opening the account has affixed his signature or thumb print, as the case may be, in his presence;

(ii) a small account shall be opened only at Core Banking Solution linked banking company branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to a small account and that the stipulated limits on monthly and annual aggregate of transactions and balance in such accounts are not breached, before a transaction is allowed to take place;

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

(iv) a small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of client shall be established through the production of officially valid documents, as referred to in sub rule (2) of rule 9"; and

(v) foreign remittance shall not be allowed to be credited into a small account unless the identity of the client is fully established through the production of officially valid documents, as referred to in sub-rule (2) of rule 9."

(Notification No.14/2010/F.No.6/2/2007- ES)

(S.R. Meena)
Under Secretary

Note: The principal rules were published in Gazette of India, Extraordinary, Part-II, Section 3, Sib-Section (i) vide number G.S.R.444 (E), dated the 1st July, 2005 and subsequently amended by number G.S.R.717 (E), dated the 13th December, 2005, number G.S.R. 389(E), dated the 24th May, 2007, number G.S.R. 816(E), dated the 12th November, 2009, number G.S.R.76 (E), dated the 12th February, 2010 and number G.S.R. 508(E), dated the 16th June, 2010.

Annexure VI (OBC KYC/AMLFY-2019-20)

"Foreign Contribution (Regulation) Act, 1976"

Obligations of banks

Master Circular of Reserve Bank of India: RBI/2004-05/388

DBOD. AML. BC. No. 74 / 14.01.055/2004-05 dated 05.03.2005

As you are aware, the provisions of Foreign Contribution (Regulation) Act, 1976 impose certain obligations on banks in respect of receipt of foreign donations. Instructions in this regard are being issued by the International Banking Division Head Office, from time to time, for ensuring scrupulous adherence to the FCRA provisions. We reproduce below the Master Circular on the provisions of Foreign Contribution (Regulation) Act, 1976, regulating receipt of foreign contributions by Associations/Organisations in India as issued by Reserve Bank of India as under:

Statutory Provisions: The Foreign Contribution (Regulation) Act, 1976 (FCRA, 1976) stipulates in terms of Section 4 ibid that no foreign contribution shall be accepted by any candidate for election; correspondent, columnist, cartoonist, editor, owner, printer or publisher of a registered newspaper; judges, government servants or employees of any corporation; members of any legislature; political party or office bearer thereof. Subsection (a) and (b) of Section 10 of the Act provide that Central Government may prohibit any association not specified in Section 4 ibid or any person from accepting any foreign contribution or require any association to obtain prior permission of the Central Government before accepting any foreign contribution. Section 5 of the above mentioned Act also provides that no organization of a political nature, not being a political party can accept foreign contribution except with the prior permission of the Central Government. The Act also provides that associations having a definite cultural, economic, educational, religious and social programme should get themselves registered with the Ministry of Home Affairs, Government of India, New Delhi before receiving any foreign contribution. Such foreign contributions should be received only through the designated bank branch the name of which has been specified in the application for registration submitted to the Ministry of Home Affairs. It is further laid down in the Act that any and every association referred to in sub-section (I) of Section (6) may, if it is not registered with the Central Government, accept any foreign contribution only after obtaining prior permission of the Central Government.

Conditions for accepting foreign donation by banks: Banks are required to strictly adhere to the provisions of FCRA,1976 while dealing with receipt of foreign contributions. It has been brought to our notice by the Government on several occasions that branches of banks are not scrupulously adhering to the provisions of the FCRA, 1976 and that foreign contributions were received by entities governed by Section 6(1) and Section 5(1), without obtaining prior permission of the Central Government.

In this connection, banks have been advised several times to scrupulously adhere to the provisions of FCRA, 1976. A list of circulars issued earlier in this regard is annexed. You are once again advised to ensure that violation of the provisions of FCRA, 1976 are avoided and procedure as indicated below is followed while receiving foreign contributions:

(a) To insist on prior permission of Central Government before accepting a foreign contribution in the accounts of entities covered under Section 4 and 5 of the FCRA, 1976;
(b) To afford credit of the proceeds of cheques/drafts representing foreign contribution only if the association etc., as indicated in Section 6 of the Act are registered with the Ministry of Home Affairs, Government of India;
(c) To insist on production of a communication from the Ministry of Home Affairs conveying prior permission of the Central Government for acceptance of specific amount of foreign contribution in case the association is not registered under the Foreign Contribution (Regulation) Act, 1976;
(d) Not to afford credit to the account of such associations as are not registered with the Ministry of Home Affairs separately for the purpose of accepting foreign contribution under the Foreign Contribution (Regulation) Act, 1976;
(e) Not to afford credit to the account of such association as have been directed to receive foreign contributions only after obtaining prior permission of the Central Government;
(f) Not to allow the credit of the proceeds of the cheques/demand drafts etc., to the organizations of a political nature, not being political parties (including their branches and units) unless a letter containing the prior permission of the Central Government under the Foreign Contribution (Regulation) Act, 1976 is produced by such organizations;
(g) To note the registration number as conveyed by the Ministry of Home Affairs to the various associations, in the relevant records particularly the pages of the ledgers in which the foreign contribution accounts of associations are maintained to ensure that no unwanted harassment is caused to such associations.

Acceptance of donation from foreign source: It is further clarified that these organizations/associations can accept contributions from a "Foreign Source" only if they are registered with the Ministry of Home Affairs or only after obtaining prior permission from the above Ministry. The "Foreign Source" for the purpose of the aforesaid Act has been defined in Section 2(e) of the Act ibid and it is evident therefrom that remittances from Indians abroad i.e. Indian citizens, for the purpose of contributing to the aforesaid associations/organizations do not attract the provisions of FCRA. However, in case of contribution given by the non-resident **foreign citizens** of Indian origin through their NRE and FCNR accounts maintained in India, the provisions of FCRA will be attracted and these contributions are to be treated as "Foreign Source". Consequently, recipient associations /organizations would require registration under FCRA or prior permission of the central Government before accepting contributions from a 'foreign source'.

Common Irregularities Observed: Some of the irregularities noticed in this regards are as under:

(a) Certain associations were found to be operating more than one account, either in the same branch or in different branches (other than the account specified in the communication for registration), for carrying on transactions of foreign contributions.

(b) Certain associations were allowed credit of cheques/drafts representing foreign contribution and withdrawal thereof without the association being registered or without its obtaining prior permission of the central government
(c) Despite the fact that copies of the orders putting an association into prohibited category or prior permission category under sub-section (a) and (b) of Section 10 the said Act were sent to the bank branches, they allowed credit/withdrawal of foreign contributions by the said associations without seeking Government's prior approval.

Periodical Reporting to Central Government: Under the existing instructions, all the branches of the bank dealing in foreign exchange are required to send a half yearly statement to Government of India for the period ending 30th September and 31st March every year as per the enclosed format giving the details of the contributions received for crediting into the account of associations/organizations concerned. Such statements are required to be furnished directly to Government of India within two months of the closure of the half year. It has been reported by the Government that banks are not furnishing the information to the Home Ministry regularly. This assumes significance as it is feared that some part of the foreign donations received through banking channels is getting diverted to fund unlawful activities. The Government of India has therefore taken a serious view of the lapses in complying with the provisions of Foreign Contribution (Regulation) Act, 1976 by banks.

Miscellaneous: Under Section 10(a) of Foreign Contribution (Regulation) Act, 1976 Government has prohibited some of the Associations / Organisations from receiving foreign contribution. Further, some organisations have been declared as being organisations of political in nature, not being a political party under section 5 of the Act ibid. Banks are requested to advise all their branches to keep a special watch on the accounts of these Associations / Organisations and any violation of the provisions of the Act by them may immediately be brought to the notice of the Ministry of Home Affairs.

****

Appendix A : Indicative List of High/Medium Risk Customers

Characteristics of High Risk Customers

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

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

Characteristics of Medium Risk Customers

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

Appendix B : Indicative List of High / Medium Risk Products Services

1. Electronic funds payment services such as Electronic cash (e.g. stored value and payroll cards), fund transfers (domestic and international), etc.
2. Electronic banking
3. Private banking (domestic and international)
4. Trust and asset management service
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 service 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. Service offering anonymity or involving third parties
17. Service involving banknote and precious metal trading and delivery
18. Service offering cash, Monetary or bearer instruments, cross-border transactions, etc.

Appendix C : Indicate List of High / Medium Risk Geographies

Countries / Jurisdictions

1. Countries subject to sanctions, embargoes or similar measures in the United Nations Security Council Resolutions ("UNSCR")
2. Jurisdictions identified in FATF public statement as having substantial money laundering and terrorist financing (ML/TF) risks (www.fatf-gafi.org)
3. Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies (www.fatf-gafi.org)
4. Tax havens or countries that are known for highly secretive banking and corporate law practices
5. Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures
6. Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations 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 experience, 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 experience, transaction history, or other factors

"Credible sources" refers to information in reports of Financial Action Task Force, FATF-style regional bodies, International Monetary Fund, World Bank, Organisation for Economic Co-operation and Development, Egmont Group of Financial Intelligence Units or similar bodies and inputs received from RBI, FIU-IND, or other competent authorities.