KYC / AML Policy – 2018

Amended upto 15.03.2018

KYC / AML Cell

Operations Department

CENTRAL OFFICE

के वाय सी - ध शो नि कक्ष, केन्द्रीय कार्यालय, अनुपालन विभाग, मुम्बई
KYC - AML Cell, Operations Department, Central Office, 2nd floor, MMO Building,
M.G. Road, Fort, Mumbai-400001. Tele: (022) 22701921-22-23-24 (Tele-fax) - 24-25-26 Fax: 22701923.

Preface

Our previous KYC / AML Policy was updated and circulated on 06.04.2017. The present KYC / AML Policy is updated by the KYC / AML Cell, Operations Department incorporating guidelines issued by Statutory/Regulatory Authorities upto 15 March 2018. The updated Policy is being placed before the field functionaries for guidance and reference while on boarding customers to our Bank as well as during conduct of the account. We trust the various procedures laid down in the policy will be scrupulously followed to avoid pitfalls and to prevent use of Banking channels for money laundering and terrorist financing.

19.03.2018 (B K Singal)
Place: Mumbai General Manager - Operations

के वाय सी - ध शो नि कक्ष, केन्द्रीय कार्यालय, अनुपालन विभाग, मुम्बई
KYC - AML Cell, Operations Department, Central Office, 2nd floor, MMO Building,
M.G. Road, Fort, Mumbai-400001. Tele: (022) 22701921-22-23-24 (Tele-fax) - 24-25-26 Fax: 22701923.

KYC - AML Policy --2018

INDEX

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

1. "KNOW YOUR CUSTOMER" NORMS.

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

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

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

1.3.1. To ensure appropriate customer identification.

1.3.2. Monitor the transactions of a suspicious nature.

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

1.3.4. Minimize the risk due to any inadvertent overdraft.

1.3.5. Satisfy that the proposed customer is not an undischarged insolvent.

1.3.6. Minimize frauds.

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

1.3.8. Weed out undesirable customer.

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

1.4.1. A person or entity that maintains an account and/or has a business relationship with the Bank.

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

The procedure for determination of Beneficial Ownership is as under:

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

के वाय सी - ध शो नि कक्ष, केन्द्रीय कार्यालय, अनुपालन विभाग, मुम्बई
KYC - AML Cell, Operations Department, Central Office, 2nd floor, MMO Building,
M.G. Road, Fort, Mumbai-400001. Tele: (022) 22701921-22-23-24 (Tele-fax) - 24-25-26 Fax: 22701923.

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

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

Explanation: Term 'body of individuals' includes societies.

(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 (15%) or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

(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.

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

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

2. CUSTOMER ACCEPTANCE POLICY (CAP)

2.1 ACCOUNT OPENING PROCEDURES

2.1.1. Any Indian National-resident / Non-resident / Partnership firms / limited companies / Trusts can open an Account with a Bank either singly or jointly with other.

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

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

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

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

i. The aggregate of all credits in a financial year does not exceed rupees one lakh;

ii. The aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and

iii. The balance at any point of time does not exceed rupees fifty thousand.

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

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

ii) A small account shall be opened only at Core Banking Solution linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the 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 to the branch of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months;

iv) A small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of customer shall be established through the production of "officially valid documents"; and

के वाय सी - ध शो नि कक्ष, केन्द्रीय कार्यालय, अनुपालन विभाग, मुम्बई
KYC - AML Cell, Operations Department, Central Office, 2nd floor, MMO Building,
M.G. Road, Fort, Mumbai-400001. Tele: (022) 22701921-22-23-24 (Tele-fax) - 24-25-26 Fax: 22701923.

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

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

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

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

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

2.1.2.5 Indicate mode of operation.

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

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

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

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

Henceforth, customers may submit only one documentary proof of address (either current or permanent) while opening a bank account while 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.

In case the proof of address furnished by the customer is not the local address or address where the customer is currently residing, the branch is to merely take a declaration of the local address on which all the correspondence will be made by

the branch with the customer. No proof is required to be submitted for such address for correspondence/local address. This address may be verified by the bank through 'positive confirmation 'such as acknowledgement of receipt of (i) letter, cheque books, ATM cards ;(ii) telephonic conversation ;(iii) visits; etc. In the event of change in this address due to relocation or any other reason, customers may intimate the new address for correspondence to the bank within two weeks of such a change.

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

2.1.2.8 Give details of other accounts with any other banks

2.1.2.9 Permanent Account Number (PAN) given by Income Tax authorities or declarations as applicable. Verification of PAN number should be done online from system/Income Tax site. **Form 60 shall be obtained from persons who do not have PAN.**

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

2.1.2.11 **Foreign Portfolio Investors (FPI)-Harmonization of KYC norms for FPI:**

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

Alternatively, branches may rely on the KYC verification done by the third party (i.e. the Custodian/SEBI Regulated Intermediary) subject to the condition laid down in rule 9(2) [(a) to (e)] of rules prescribed in Para3.2.3.1 hereafter.

In this regard, custodians/Intermediaries regulated by SEBI may share the relevant KYC documents with the branch concerned based on written authorization from the FPIs. Accordingly, a set of hardcopies of the relevant KYC documents furnished by the FPIs to the Custodians/ Regulated Intermediaries may be transferred to the concerned branch through their authorized representative. While transferring such documents, the Custodian/ Regulated Intermediary shall certify that the documents have been duly verified with the original or notarized documents have been obtained, where applicable. In this regard, a proper record of transfer of documents, both at the level of the Custodian/Regulated Intermediary as well as at the branch, under signatures of the officials of the transferor and transferee entities, may be kept. While opening accounts for FPIs in terms of the above procedure, branches may bear in mind that they are

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

It is further advised that to facilitate secondary market transactions, the branch may share the KYC documents received from the FPI or certified copies received from a Custodian/Regulated Intermediary with other banks/ regulated market intermediaries based on written authorization from the FPI.

These provisions are applicable for both new and existing FPI clients. These provisions are applicable only for Portfolio Investment Scheme (PIS) by FPIs. In case the FPIs intend to use the account opened under the above procedure for any other approved activities (i.e. other than PIS), they would have to undergo KYC drill as per RBI master circular on Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002.

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

a) Foreign students arriving in India, who are not able to provide an immediate address proof while approaching a bank for opening bank account may be allowed to open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with appropriate visa & immigration endorsement) which contains the proof of identity and address in the home country along with a photograph and a letter offering admission from the educational institution.

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

c) During the 30 days period, the account should be operated with a condition of allowing foreign remittances not exceeding USD 1,000 into the account and a cap of monthly withdrawal to Rs.50,000/-, pending verification of address.

d) On submission of the proof of current address, the account would be treated as a normal NRO account and will be operated in terms of the instructions contained in RBI's instructions on Non-Resident Ordinary Rupee (NRO) account and the provisions of Schedule 3 of FEMA Notification 5/2000 RB dated May 3, 2000 and the amendment made thereafter in relevant provisions of RBI/ FEMA.

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

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

2.1.2.14 **Self Help Group – KYC procedure for opening of bank accounts**

a) **KYC verification of all the members of SHG is not required while opening the saving bank account of the SHG.**
b) **KYC verification of all office bearers shall suffice.**
c) **No separate KYC verification of the members or office bearers shall be necessary at the time of credit linking of SHGs.**

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

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

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

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

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

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

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

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

2.2. PRECAUTIONS TO BE TAKEN

While opening the account it should be ensured that:-

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

2.2.2. No account should be opened where the bank is unable to verify the identity and/or obtain documents required or non-reliability of the data/information furnished to the bank.

2.2.3. Before opening a new account, it should be ensured that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc. The Branches should refer the circulars issued by RBI/Government of India/Central Office from time to time wherein the names of banned/terrorist individuals/organization etc. are notified. The name(s) of the prospective customer should be verified with the latest "List of Terrorist Individuals/Organization under UNSCR 1267(1999) and 1822(2008) on Taliban/Al-Qaida Organization" available at Bank's **ftp server and the path - ftp://centftp.cbi.co.in/public/aml**

2.2.4. In cases where the customer is permitted to act on behalf of another person/entity the circumstances should be clearly spelt out in conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity.

2.2.5. The branches should prepare the customer profile of the customer which should contain information relating to customers' identity, social/financial status, nature of business activity, information about his clients' business and their location etc. **and risk categorization shall be undertaken based on these parameters. While considering customer's identity, the ability to confirm identity documents through online or other services offered by the issuing authorities may also be factored in.** The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

2.2.6. The customer profile shall be prepared based on risk categorization, as defined below:

2.2.6.1. **Low Risk Category**: Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile.
Example:
a) Salaried Employees, whose salary structures are well defined,
b) People belonging to lower economic strata of the Society whose accounts show small balances and low turnover,
c) Government departments and Government owned Companies, Regulators and statutory bodies etc.
For low risk category customers, only the basic requirements of verifying the identity and location of the customer are to be obtained. However, whenever there is suspicious of money laundering or terrorist financing or when other factors give rise to a belief that the customer does not, in fact pose a low risk,

के वाय सी - ध शो नि कक्ष, केन्द्रीय कार्यालय, अनुपालन विभाग, मुम्बई
KYC - AML Cell, Operations Department, Central Office, 2nd floor, MMO Building,
M.G. Road, Fort, Mumbai-400001. Tele: (022) 22701921-22-23-24 (Tele-fax) - 24-25-26 Fax: 22701923.

full scale customer due diligence should be carried out before opening an account or whenever such risk perceived.

2.2.6.2. **High Risk Category**: Individuals and entities whose identities and sources of funds are not clear and cannot be easily identified.
Example:
a) Non-resident customers
b) High Net Worth individuals
c) Trusts, Charities, NGOs and Organizations receiving donations
d) Companies having close family shareholding or beneficial Ownership
e) Firms with 'Sleeping Partners'
f) Politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which PEP is the ultimate beneficial owner;
g) Non face to face customers and
h) Those with dubious reputation as per public information available etc.
i) Customers dealing in antique goods
j) Money Exchange Bureaus
k) Diamond, Bullion Dealers & Jewellers
l) Arms and Ammunition dealers
However, NPOs/NGOs promoted by United Nations or its agencies may be classified as low risk customers.

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

2.2.6.3 **Medium Risk Category** are those individuals who live in Medium risk Countries i.e. all Countries in Africa and all countries in the America other than USA and Canada and Such customers who possess lower risk than 'High Risk Customers' but higher than the 'Low Risk Customers' based on their background, nature and location of activity, country of origin, sources of funds etc. The Risk Classification may be lower for those customers where sufficient knowledge in the public domain is available to Bank (e.g. listed companies, Regulated Entities).

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

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

3. CUSTOMER IDENTIFICATION PROCEDURE (CIP)

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

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

(a) while establishing a banking relationship;
(b) carrying out a financial transaction and
(c) when the bank has a doubt about the authenticity / veracity or the adequacy of the earlier obtained customer / identification data.

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

3.1 IDENTIFICATION OF CUSTOMER

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

3.1.1 WHAT IS IDENTITY?

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

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

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

3.1.1.1. **Natural Person:** A natural person's identity comprises his name and all other names used, the date of birth, and an address/location at which he/she can be located and also his/her recent photograph.

3.1.1.2. **Legal Person:** The legal status of the legal person/entity should be verified through proper and relevant documents; verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person; understand the ownership and control structure of the customer and determine who are the natural person(s) who ultimately control the legal person.

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

3.1.2 WHAT IS IDENTIFICATION ?

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

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

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

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

Features	Documents
Accounts of Individuals • Legal name and Any other names used • Correct permanent address	Officially valid documents :- 1. Passport, 2. Driving license, 3. Permanent Account Number (PAN) Card, 4. Voter's Identity Card issued by Election Commission of India, 5. Job card issued by NREGA duly signed by an officer of the State Government, 6. Letter issued by the Unique Identification Authority of India containing details of name, address. 7. Any document as notified by the Central Government in consultation with the Regulator. It is implied that proof of address also follows from the above documents only. A document shall be deemed to be an 'Officially Valid Document' even if there is a change in the name subsequent to its issuance, provided it is supported by a marriage certificate issued by the State Government or a Gazette notification indicating such a change of name, while establishing an account based relationship or during periodic updation exercise, for persons whose name is changed due to marriage or otherwise.

	Henceforth, only the said documents mentioned in PML rules or any other documents as notified by the Central Government in consultation with the Regulator would be 'Officially valid documents' The discretion given to banks earlier stands withdrawn. 'Simplified measures' may be applied in the case of 'Low risk' customers taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved. In respect of low risk category of customers, where simplified measures are applied, it would be sufficient to obtain any of the following documents i. 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; ii. letter issued by a gazetted officer, with a duly attested photograph of the person. For the limited purpose of proof of address, the following additional documents will be deemed to be OVDs under 'simplified measures'. (a) Utility bill which is not more than two months old of any service provider (electricity, telephone, postpaid mobile phone, piped gas, water bill); (b) Property or Municipal Tax receipt; (c) Bank account or Post Office savings bank account statement; (d) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; (e) 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 (f) Documents issued by Government departments of foreign jurisdictions **or** letter issued by Foreign Embassy or Mission in India. The additional documents mentioned above shall be deemed to be OVDs under 'simplified measure' for the 'low risk' customers for the limited purpose of proof of address, where customers are unable to produce any OVD for the same.

के वाय सी - ध शो नि कक्ष, केन्द्रीय कार्यालय, अनुपालन विभाग, मुम्बई
KYC - AML Cell, Operations Department, Central Office, 2nd floor, MMO Building,
M.G. Road, Fort, Mumbai-400001. Tele: (022) 22701921-22-23-24 (Tele-fax) - 24-25-26 Fax: 22701923.

Accounts of Companies • Name of the Company • Principal place of Business. • Mailing address of the company • Telephone/Fax Number	a) Certificate of incorporation; b) Memorandum and Articles of Association; c) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and d) An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf.
Accounts of Proprietorship concerns: Proof of Identity and Address for Proprietor along with	1. Proof of name, address and activity of the concern like Registration Certificate (In the case of registered concern). 2. Certificate/license issued by Municipal Authorities under Shop & Establishment Act. 3. Utility bills such as electricity, water and landline telephone bills in the name of the proprietary concern. 4. Sales return 5. The complete Income tax return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax Authorities. 6. **GST registration.** 7. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. 8. Registration/licensing document issued in the name of the proprietary concern by the Central Government or State Government authority/Department. 9. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of bank account. 10. License issued by Registration authorities like Certificate of Practice issued by the Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food & Drug Control Authorities etc. Any of two of the above documents would suffice. These Documents should be in the name of the proprietary concern. It has been clarified that though the default rule is that any two documents should be provided as activity proof, in case where the Branch is satisfied that it is not possible to furnish two such documents, then it will have the discretion to accept only one of the specified documents as activity proof. However the Branch will have to undertake contact point verification and collect such information as would be required to establish the existence of such firm and confirm, clarify and satisfy itself that the business activity has been

	verified from the address of the proprietary concern. After proper verification of the business activity and the address of the proprietary concern, a physical record of the contact point verification should be maintained along with the other KYC documents of the customer. It is further clarified that the list of registering authorities indicated above are only illustrative and therefore will also include license/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under the statute as one of the documents to prove the activity of the proprietary concern.
Accounts of Partnership firms	One certified copy of each of the following: a) Registration certificate; b) Partnership deed; and c) An officially valid document in respect of the person holding an attorney to transact on its behalf.
Accounts of Trusts & Foundation	One certified copy of each of the following: a) Registration certificate, b) Trust deed, and c) An officially valid document in respect of the person holding power of attorney to transact on its behalf.
Unincorporated Association or Body of Individuals	One certified copy of each of the following: a) Resolution of the managing body of such association or body of individuals; b) Power of attorney granted to him to transact on its behalf; c) An officially valid document in respect of the person holding an attorney to transact on its behalf; and d) Such information as may be required by the branch to collectively establish the legal existence of such an association or body of individuals.
Juridical Persons: Government or its departments, Societies, Universities and Local bodies like Village Panchayats	**One certified copy of the following:** a) **Documents showing name of person authorized to act on behalf of the entity;** b) **Officially valid documents for proof of identity and address in respect of the person holding an attorney to transact on its behalf; and** c) **Such documents as may be required by the branch to establish the legal existence of such an entity / juridical person.**

3.1.2.5 Salaried Persons:

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

identity as well as address proof. Such a practice is open to misuse and fraught with risk. Branches should insist on at least one of the officially valid documents as provided in the PML Rules (viz. passport, driving license, PAN card, Aadhar Card and Voter's Identity card etc.) or the documents for KYC purposes prescribed in para 3.1.2 for customers where 'Simplified measures' are applied, to open account of salaried employees of corporate and other entities.

3.1.2.6 Opening of accounts by close relatives:

In cases of close relatives, e.g. wife, son, daughter and parents etc. who live with their husband, father/mother and son as the case may, branches can obtain an identity document and utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) wanting to open an account is a relative and is staying with him/her.

3.1.2.7 Full operational facilities in joint account with spouse staying at separate stations:

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

3.1.2.8 Accounts portability/opening of new Bank Accounts:

Branches are advised that KYC once done by one branch should be valid for transfer of the account within the bank as long as full KYC has been done for the concerned account. The customer should be allowed to transfer his account from one branch to another branch without restrictions. Branches may transfer existing accounts at the transferor branch to the transferee branch without insisting on fresh proof of address and on the basis of a self-declaration from the account holder about his/her current address.

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.

3.1.2.9 Accounts of migratory workers:

The migratory workers experienced difficulties in opening of bank accounts at a location other than their permanent place of residence, mainly because it is insisted to provide proof of residence of the locality of the bank branch, whereas, no such insistence is required as per RBI guidelines. The branches opening such an account may get the details of permanent place of residence verified through an 'on-line' communication to nearest branch of the permanent domicile within 30 days of opening of an account, within which the customer may be allowed limited operations to enable him/her meet basic day-to-day requirement of funds.

3.1.2.10 Accounts of Politically Exposed Persons (PEPs) resident outside India:

a. 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. **The identity of the person is to be verified before accepting PEP as the customer.** The decision to open an account for PEP should be taken at a senior level. Branches should also subject such accounts to enhanced monitoring on an ongoing basis. Sufficient information including information about the sources of funds, accounts of family members and close relatives is to be gathered on the PEPs. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

b. 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. In this connection the Branch Manager in case of Scale IV and above Branches and Regional Managers in case of Branches up to Scale III are the competent authority to take decision to open an account of PEPs. These instructions are also applicable to accounts where PEP is the ultimate beneficial owner.

c. Further, branches should have appropriate ongoing risk management procedures for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which PEP is the ultimate beneficial owner.

3.1.2.11 Accounts of non-face-to-face customers**: Non-face-to-face customer means customers who opened accounts without visiting the branch /offices or meeting the officials.**

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. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented should be insisted upon and, if necessary, additional documents may be called for. 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 bank 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.

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

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

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

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

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

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

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

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

A walk-in customer at a bank branch can remit funds up to Rs.50,000 to the bank account of a beneficiary through NEFT. Besides, banks are also permitted to allow such customers to transfer funds to a Bank account of a beneficiary through BCs, ATMs, etc. up to a maximum amount of Rs.5,000 per transaction with a monthly cap of Rs.25,000. Such a walk-in customer needs to provide minimum details like his name and complete address to the remitting bank.

3.1.3 WHAT IS VERIFICATION?

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

3.1.4 VERIFICATION OF CREDENTIALS/ANTECEDENTS:

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

3.1.5 FORMALITIES FOR OPENING OF ACCOUNT:

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

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

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

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

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

3.1.5.6. **Periodical Updation of KYC**:

Branches should carry out periodical updation of KYC information of every customer, which may include the following:

i) Full KYC exercise may be done at least every two years for high risk customers, every eight years for medium risk customers and every ten years for low risk customers. Full KYC may include all measures for confirming identity and address and other particulars of the customer that the branch may consider reasonable and necessary based on the risk profile of the customer. Branches need not seek fresh proofs of identity and address at the time of periodic updation, from those customers who are categorized as 'low risk', in case of no change in status with respect to their identities and addresses. A self-certification by the customer to that effect should suffice in such cases. In case of change of address of such 'low risk' customers, they could merely forward a certified copy of the document (proof of address) by mail / post, etc. branch may not insist on physical presence of such low risk customer at the time of periodic updation.

ii) Fresh photographs to be obtained from minor customer on becoming major.

iii) Carry out ongoing due diligence of existing customers in order to ensure that their transactions are consistent with the branch's knowledge of the customer, his business and risk profile and wherever necessary, the source of funds.

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

v) e-KYC process using OTP based authentication for purpose of periodic updation is allowed, provided, while onboarding the customer was subjected to KYC process as prescribed in Para 2.1.

3.2 Customer Due Diligence (CDD) :

The customer due diligence **means identifying and verifying the customer and the beneficial owner using 'Officially Valid documents' as a 'proof of identity' and a 'proof of address'.** It may be defined as any measure undertaken by a financial institution to collect and verify information and positively establish the identity of a customer. **While opening a joint account, CDD procedure is to be followed for all the joint account holders.**

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

3.2.1 Basic Due Diligence:

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

3.2.2 Simplified Due Diligence:

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

3.2.3 Enhanced Due Diligence (EDD):

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

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

3.2.3.1 Client accounts opened by professional intermediaries:

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

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

(a) The Branch immediately obtains necessary information of such client due diligence carried out by the third party;

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

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

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

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

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

3.2.3.2 Accounts of Politically Exposed Persons (PEPs) resident outside India as defined in Para No.3.1.2.10

3.2.3.3 Accounts of non-face-to-face customers as defined in Para No.3.1.2.11

3.2.3.4 **Correspondent Banking**

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable through-accounts, cheques clearing etc. Branches should gather sufficient information to understand fully the nature of the business of the correspondent/ respondent bank. Information on the other bank's 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 correspondent's/respondent's country may be of special relevance. Similarly, Branches should try to ascertain from

publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. While it is desirable that such relationships should be established only with the approval of the Board**,** in case the Boards of some banks wish to delegate the power to an administrative authority, they may delegate the power to a committee headed by the Chairman/CEO of the bank while laying down clear parameters for approving such relationships. Proposals approved by the Committee should invariably be put up to the Board at its next meeting for post facto approval. The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented. 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. The correspondent bank should also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

3.2.3.5 **Nonresident Indians (NRIs)/Foreign Nationals**

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

3.2.3.6 **Fiduciary Accounts**

Bank may exercise enhanced due diligence at the time of opening fiduciary accounts by intermediaries such as guardians of estates executors, administrators, assignees, receivers etc. for e.g. while opening of the account of an administrator of the estate, it may be necessary to examine the Letter of Administration (Authority) as it would give a picture of the assets of the estate.

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

Branches have arrangements with co-operative banks wherein the latter open current accounts and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in- customers for facilitating their remittances and payments. Since the 'at par' facility offered by commercial banks to co-operative banks is in the nature of Correspondent banking arrangements, branches should monitor and review such arrangements to assess the risks including credit risk and reputational risk arising therefrom. For this purpose, branches should retain the right to verify the records maintained by the client cooperative banks/ societies for compliance with the extant instructions on KYC and AML under such arrangements.

3.3 Correspondent relationship with a "Shell Bank":

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

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

3.3.3 Applicability 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.

3.4 Information sought by Banks from Customers

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

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

3.4.3 Other 'optional' customer details/additional information, if required may be obtained separately after the account is opened only with the explicit consent of the customer. The customer has a right to know what is the information required for KYC that she/he is obliged to give, and what is the additional information sought by the bank that is optional.

3.4.4. Further, it is reiterated that branches should ensure that the information (both 'mandatory' – before opening the account as well as 'optional'-after opening the account with the explicit consent of the customer) collected from the customer is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes.

3.5 <u>e-KYC Service of UIDAI – Recognizing on-line Aadhaar authentication (electronic verification process) to be accepted as an' Officially Valid Document' under PML Rules</u>

3.5.1 In order to reduce the risk of identity fraud, document forgery and have paperless KYC Verification, Branches shall utilize the e-KYC service provided by UIDAI.

3.5.2 e-KYC service has been accepted as a valid process for KYC verification under Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

3.5.3 The information containing demographic details and photographs made available from UIDAI as a result of e-KYC process ("which is in an electronic form and accessible so as to be usable for a subsequent reference") may be treated as an 'Officially Valid Document' under PML Rules. Branches may accept e-Aadhar downloaded from UIDAI website as an officially valid document subject to the following:-

a) If the prospective customer knows only his/her Aadhaar number, the branch may print the prospective customer's e-Aadhaar letter in the branch directly from the UIDAI portal, **provided, the prospective customer is physically present in the branch.**

b) If the prospective customer carries a copy of the e-Aadhaar downloaded elsewhere, the branch may print the prospective customer's e-Aadhaar letter in the branch directly from the UIDAI portal or confirm identity and address of the resident through simple authentication service of UIDAI.

3.5.4 In this connection, it is advised that while using e-KYC service of UIDAI, the individual user has to authorize the UIDAI, by explicit authentication (biometric) to the bank branches/business correspondents (BCs).The UIDAI then transfers the data of the individual comprising name, age, gender, and photograph of the individual, electronically to the bank/BCs, which may be accepted as valid process for KYC verification.

3.5.5. Physical Aadhaar card/letter issued by UIDAI containing details of name, address and Aadhaar number received through post would continue to be accepted as an 'Officially Valid Document'.

3.6 Closure of KYC Non-Compliant Accounts - Competent Authority for Approval:

Branches are advised to strictly adhere the guidelines on KYC/AML and to:

3.6.1 Follow up personally on telephone/e-mail/sms alerts or other means of communication, to contact the customer, obtain the KYC documents and update the same in relevant fields in the CBS System.

3.6.2 If there is no response from the customer, as an initial measure, his account may be kept under close watch for a period not extending three months, by providing the basic banking facilities to these customers. Any additional facilities available to KYC compliant customer will no more be available to such customer till he provides the necessary documents.

3.6.3 If there is no response from the customer despite repeated reminders, his account may be kept under close watch and Branch should impose 'Partial freezing' on such KYC non-compliant account in a phased manner. Meanwhile, the account holders can revive accounts by submitting the KYC documents as per instructions in force. While imposing 'Partial freezing', branches are advised to ensure that the option of 'Partial freezing' is exercised after giving due notice of three months initially to the customers to comply with KYC requirement and followed by a reminder for further period of three months. Thereafter, branch may impose 'Partial freezing' by allowing all credits and disallowing all debits with the freedom to close the accounts. If the accounts are still KYC non-compliant after six months of imposing initial 'Partial freezing' branch may disallow all debits and credits from / to the accounts, rendering them inoperative. Further, it would always be open to the branch to close the account of such customers.

The sanctioning authority to approve the partial freezing, rendering the account inoperative and closure of such KYC non-compliant account will be as follows:

Category of Branch	Sanctioning Authority
Small, Medium, Large	Chief Manager/Assistant General Manager at Regional Office
Very Large, Extra Large, Exceptionally Large	Deputy Zonal Manager (second in Command/Zonal Manager at Zonal Office

When an account is closed either without 'partial freezing' or after 'partial freezing' the reason for closure shall be communicated to the account holder.

3.7 Guidelines on Unique Customer Identification Code (UCIC)

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

3.7.2 To start with, it is proposed for introduction of unique identifiers for customers within the Bank. In our bank CIF is the Unique Number of customers.

3.7.3 The existing customers having multiple CIFs will be consolidated by the exercise of de-duplication.

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

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

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

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

4 REPORTING REQUIREMENT UNDER FATCA AND CRS

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

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

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

5. ANTI MONEY LAUNDERING STANDARDS

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

The technological advancements have facilitated on line transfer of funds and real time settlement between the Banks across the globe. This has helped money launderers to adopt innovative means and move funds faster across continents making detection and preventive action much more difficult. This calls for a dynamic approach in tracking the crime. The staff members of the Bank must be vigilant in the fight against money laundering and must not allow the bank to be used for money laundering activities. The Bank should not become the party to violation of law. As such, preventing money laundering activities is the duty and responsibility of the bank staff.

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

5.1 MONEY LAUNDERING:

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

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

activities relating to a scheduled offence or the value of such property. Money Laundering, therefore, besides being a Statutory or Regulatory requirement is also a moral responsibility for all the Bank Employees.

Nomination of Designated Director:

Banks are required to nominate a Director on their Boards as "Designated Director", as per the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Rules), to ensure overall compliance with the obligations under the Act and Rules.

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

Principal Officer:

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

5.2 TERRORIST FINANCING:

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

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

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

5.3 WIRE TRANSFERS:

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.

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

a) Wire transfer is 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. 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 affect 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.

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

(A) CROSS BORDER WIRE TRANSFERS.

i) All cross-border wire transfers 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.

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.

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

5.3.3 EXEMPTIONS

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

5.3.4 ROLE OF ORDERING, INTERMEDIARY AND BENEFICIARY BANKS:

(a) Ordering Bank

An ordering bank is the one that originates a wire transfer as per the order placed by its customer. If the branch is an ordering bank, it must ensure that qualifying wire transfers contain complete originator information. The branch 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. If the branch is an intermediary Bank, it must be ensured that all the records as aforesaid are preserved for a period of **five** years. For further details, please refer to para 10.5 "PRESERVATION OF RECORDS" of this Policy.

(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.

5.4 CHECK LIST FOR PREVENTING MONEY-LAUNDERING ACTIVITIES

The illustrative checklist for preventing money-laundering activities is as under:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6. MONITORING OF TRANSACTIONS:

To obviate the scope for frauds and prevent Money Laundering, regular monitoring and supervision of accounts is essential. By understanding the normal and reasonable activity of the customers, coupled with controlling the accounts effectively, risk can be reduced. Monitoring customer activity and transactions throughout the relationship helps the Banks to know their customers, assess risk and provides greater assurance that the Bank is not being used for the purposes of financial crime. However, the extent of monitoring will depend on the non-sensitivity of the account. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. Special attention should be paid to the complex, unusually large transactions and all unusual patterns which have no apparent economic or lawful purpose.

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

(i) Opening of an account;

(ii) Deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;

(iii) The use of a safety deposit box or any other form of safe deposit;

(iv) Entering into any fiduciary relationship;

(v) Any payment made or received in whole or in part of any contractual or other legal obligation;

(vi) Establishing or creating a legal person or legal arrangement.

6.1 MONITORING OF CASH TRANSACTIONS:

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

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

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

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

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

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

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

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

6.2 Monitoring of other transactions

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

6.2.2 **Branches shall closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies.**

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

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

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

7. Combating Financing of Terrorism

7.1 As and when list of individuals and entities approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) are received from Government of India / Reserve Bank of India, the same are circulated to all the offices with instructions to ensure the consolidated list of individuals and entities as circulated by Reserve Bank of India is updated. The updated list of such individuals/groups/undertakings/entities associated with Al-Qaida ("Al-Qaida Sanctions list") can be accessed in the United Nations' website at http://www.un.org/sc/committees/1267/aq Sanctions list.shtml. and the updated list of such individuals associated with Taliban and entities and other groups and undertakings associated with Taliban ("1988 Sanctions list") can be accessed in the United Nations' website at http://www.un.org/sc/committees/1988/list.shtml. Branches are advised that before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the list. Further, branches should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to Compliance Officer at ROs / Principal Officer for onward submission to Reserve Bank of India / FIU-IND.

7.2 In terms of PMLA Rules, suspicious transaction should include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. Banks are, therefore, advised to develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.

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

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

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

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

Further, there should be ongoing monitoring. The background and purpose of transactions with persons (including legal and other financial institutions) as mentioned above, should be examined and if it appears that such transactions have no apparent economic or visible lawful purpose, the background and purpose of the transactions should be examined, findings to be recorded and all documents and the written findings should be retained and made available to Reserve Bank of India /other authorities, on request.

7.4 What is Suspicious Transaction ?

As per PMLA, suspicious transaction means a transaction **including an attempted transaction,** whether or not made in cash, which to a person acting in good faith:

a) gives rise to reasonable ground of suspicion that it may involve the proceeds of a crime **regardless of the value involved** or

b) appears to be made in circumstances of unusual or unjustified complexity;

c) appears to have no economic rationale or bonafide purpose;

d) gives rise to reasonable ground of suspicion that it may involve financing of activities of terrorism

e) Further, when the branch is unable to verify the identity and / or obtain documents required or non-reliability of the data /information furnished to the Bank and is unable to apply appropriate customer due diligence measures and therefore believes that it would no longer be satisfied that it knows the true identity of the customer, besides taking a decision whether to continue the business relationship, should also file an STR with FIU-IND.

Branches need to have regard to the indicators of suspicion, to determine whether or not a transaction is suspicious. An Indicative list of suspicious activities is given hereunder:

7.4.1 AN INDICATIVE LIST OF SUSPICIOUS ACTIVITIES

Transactions Involving Large Amount of Cash

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

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

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

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

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

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

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

Transactions that do not make Economic Sense

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

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

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

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

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

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

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

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

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

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

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

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

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

7.4.3.3 An account where there are several cash deposits/withdrawals below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

7.4.4. Unusual activities

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

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

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

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

7.4.5. Customer who provides insufficient or suspicious information

7.4.5.1 A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors, or its locations. In this case account need not be opened.

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

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

7.4.6. Certain suspicious funds transfer activities

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

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

7.4.7 Operation of bank accounts & Money Mules:

7.4.7.1 "Money mules" can be used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "money mules." In some cases these third parties may be innocent while in others they may be having complicity with the criminals.

7.4.7.2 In a money mule transaction, an individual with a bank account is recruited to receive cheque deposits or wire transfers and then transfer these funds to accounts held on behalf of another person or to other individuals, minus a certain commission payment. Many a times the address and contact details of such mules are found to be fake or not up to date, making it difficult for enforcement agencies to locate the account holder. Sometimes transactions related to money laundering or terrorist financing are carried out through **Money Mules.**

7.4.7.3 The operations of such mule accounts can be minimized if branches strictly follow the guidelines of KYC/AML/CFT /Obligation of banks under PMLA, 2002 issued from time to time and to those relating to periodical updation of customer identification data after the account is opened and also to monitoring of transactions in order to protect themselves and their customers from misuse by such fraudsters.

7.4.8. Certain bank employees arousing suspicion

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

7.4.8.2 An employee who is reluctant to take a vacation.

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

7.4.8.4 Negligence of employees/willful blindness is reported repeatedly.

7.4.9 SOME EXAMPLES OF SUSPICIOUS ACTIVITIES/TRANSACTIONS TO BE MONITORED BY

THE OPERATING STAFF:

7.4.9.1 Large Cash Transactions.

7.4.9.2 Multiple accounts under the same name.

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

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

7.4.9.5 Large deposits immediately followed by wire transfers.

7.4.9.6 Sudden surge in activity level.

7.4.9.7 Same funds being moved repeatedly among several accounts.

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

7.4.9.9 Transactions inconsistent with the purpose of the account.

7.4.9.10 Maintaining a low or overdrawn balance with high activity.

7.5 ISSUE/PAYMENT OF DD/TT ETC., SALE OF GOLD COINS AND SALE OF THIRD PARTY PRODUCTS

In order to curb the misuse of banking channels for violation of fiscal laws and evasion of taxes, Demand Drafts, Telegraphic transfers, Sale of Gold Coin and Third Party Products for Rs. 50,000/- and above should be issued only by debit to the customer's account or against cheque or other instruments tendered by the purchaser and not against cash payment. Similarly, payments against Demand Drafts, Telegraphic Transfer, Sale of Gold Coin and Third Party Products for Rs. 50,000/- and above should be made through banking channels only and not in cash. All the transactions carried out by a single customers during a day should be aggregated to arrive the ceiling of Rs.50000/-.

8. REPORTING SYSTEM UNDER PMLA

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

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

8.1.1 Cash Transaction Report (CTR):

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

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

8.1.2 Non-Profit Organization Transaction Report (NTR)

Bank is required to submit details of:

(a) All cash transactions involving receipts of value more than Rs.10 lakhs or its equivalent in foreign currency by clients who are non-profit organizations.
(b) NTRs must contain details of legal persons as per definition under Rule 2(1) (ca) of the Money Laundering (Maintenance of Records) Rules, 2005. Non-profit organization 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**.
(c) Transactions of an account should be given in report along with details of the legal entity, individuals, account and transaction on lines similar to those for CTRs.
(d) The report is to be filed in the format prescribed by FIU-IND
(e) NTR for every month should be submitted to FIU-IND, **by the 15th of the succeeding month.**

8.1.3 Counterfeit Currency Report (CCR):

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

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

8.1.4.1 All suspicious transactions whether or not made in cash, should be reported within 7 days of arriving at a conclusion that any transaction is of suspicious nature. It should be ensured that there is no undue delay in arriving at a conclusion whether or not a transaction is of suspicious nature and that the principal officer should record his reasons for treating any transaction or a series of transactions as suspicious nature.

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

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

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

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

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

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

While furnishing of information to the Director FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a misrepresented transaction beyond the time limit as specified in this rule shall constitute a separate violation.

8.1.7 **Attempted Money Laundering Transactions:**

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

8.1.8 **Need to file Repeat STR:**

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

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

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

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

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

8.1.10 **Tipping off the customer:**

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

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

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

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

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

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

8.1.11 **Procedure of STR Alerts scrutiny:**

8.1.11.1 The STR alerts, based on scenarios, are generated through AML software (AML system). A team of front line officers at AML-KYC Cell are screening the generated STR alerts. After first level checking by a Senior Manager and second level checking by Chief Manager, the suspicious alert shall be put up before the Principal Officer for his approval to file an STR to FIU-IND by AML Cell, CO, uploaded electronically on its FINnet site.

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

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

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

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

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

v. There is cyclic movement of funds between different parties

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

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

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

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

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

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

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

8.1.11.2 In case of exigencies the STR alerts will be decentralized to all the Regions (presently 59) for screening.

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

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

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

8.1.12 Measures for improvement of screening of STR alerts

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

a) The STR alerts screening may be partially decentralized at RO level.

b) By adopting the above method the manpower and man hours will be saved which can be utilized for monitoring and follow up.

9. RISK MANAGEMENT

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

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

10. INTERNAL CONTROL

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

10.1. Internal Audit/Inspection

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

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

10.2. Terrorism Finance:

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

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

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

10.3 Threshold Limit for monitoring of transactions:

In a broader sense threshold limit is the Annual Income/Turnover given by customers in his account and fixed by the Branch Manager. Where the same is not available, the criteria will be threshold value decided by the BMs in case of new accounts and credit summations in case of old accounts (i.e. in case of accounts of more than one year old, threshold value will be the sum total of all credits in last financial year).

To maintain uniformity in all the branches the following threshold limit per transaction is fixed which shall be subject to review from time to time.

Threshold limits for Saving Accounts:

Category of Branch	Low Risk Accounts	Medium Risk Accounts	High Risk Accounts
Rural	75000	50000	25000
Semi Urban	100000	75000	50000
Urban	150000	100000	75000
Metro	200000	150000	100000

Threshold limits for CD/Partnership/other Accounts:

Category of Branch	Low Risk Accounts	Medium Risk Accounts	High Risk Accounts
Rural	150000	100000	50000
Semi Urban	200000	150000	100000
Urban	300000	200000	150000
Metro	400000	300000	200000

The Branches shall monitor the transactions in each account as per the threshold for various categories of accounts.

10.3.1 STR reported accounts

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

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

10.3.2 Correspondent Banking

10.3.2.1 Transactions conducted through the correspondent relationships need to be managed taking a risk based approach. Know Your Correspondent procedure should be established to ascertain whether the correspondent bank or counter party is itself regulated for money laundering prevention and, if so, whether the correspondent is required to verify their customer identity to FATF standards.

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

10.4 Scenarios for generation of STR alerts:

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

10.5. <u>Preservation of Record</u>

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

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

10.5.3 Branches should ensure that records pertaining to the identification of the 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, are properly preserved for at least five years after the business relationship is ended as required under Rule 10 of the rules.

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

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

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

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

10.5.6 The records pertaining to transaction and identification as mentioned above should be made available to the competent authorities upon request.

10.6. COMPLIANCE OFFICER/MONEY LAUNDERING REPORTING OFFICER (MLRO)

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

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

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

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

****

ANNEXURE- I

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

KNOW YOUR CUSTOMER (KYC)			
Sr. No.	**DO's**	**Sr. No.**	**DON'Ts**
1	Before opening any new account, it is ensured that the prospective account opener's identity does not match with any person with known criminal background, and his name does not appear in the list of terrorist individuals/ organizations banned by UN Security Council Sanction Committee as circulated by RBI.	1	Do not open account in anonymous or fictitious / benami name(s).
2	All the copies of supporting documents given by the customer must be verified with original documents.	2	Do not accept new customer for banking relationship without application of Customer Due Diligence (CDD) measures such as location of business activity / profession, purpose of the account, social and financial status source of funds etc.
3	All transactions of suspicious nature, should be monitored	3	Do not open any account without a. Proof of Identity and Address. **Individuals** – Passport, Driving License PAN, Voter ID, Job Card issued by NREGA duly signed by officer of State Govt., Letter or Aadhaar No. issued by UIDAI containing details of name, address & aadhar number and e-KYC service of UIDAI, any document as notified by the Central Government in consultation with the regulator. **Partnership Firm** – Registration certificate, Partnership Deed, An officially valid document in respect of the person holding an attorney to transact on its behalf. **Companies** – Certificate of Incorporation, Memorandum and Articles of Association, Resolution of Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf, An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf. **Trusts &Foundations**-Registration certificate, Trust Deed and An officially valid document in respect of the person holding a power of attorney to transact on its behalf. **Unincorporated Association or Body of Individuals**-Resolution of the managing body of such association or body of individuals, Power of attorney granted to transact on its behalf, An officially valid document in respect of the person holding an attorney to transact on its behalf and Any such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals.

			Juridical Persons: Government or its department, Societies, Universities and Local bodies like Village Panchayats - Documents showing name of person authorized to act on behalf of the entity; Officially valid document for proof of identity and address in respect of the person holding an attorney to transact on its behalf and Such documents as may be required by the branch to establish the legal existence of such an entity / juridical person.
4	High risk accounts are subject to intensive monitoring and special attention is paid to all complex, usually large transactions which have no economical / lawful purpose.	4	Do not open an account without : Proof of either current or permanent address And any one of the officially valid documents.
5	Based on the risk perception, every new customer should be categorized into low, medium or high risk for monitoring purpose. Risk profiles of customers should be reviewed, once in every six months.	5	In the case of 'Small Accounts', if the balance (in all the accounts taken together) exceeds Rs. 50,000/- or total credits (in all the accounts taken together) exceeds Rs.One lac in a year, or aggregate of all withdrawals and transfers in a month exceeds Rs.Ten thousand then do not permit further transactions in the account until full KYC procedure is completed.
6	Periodical updation of KYC information of every customer (including photographs) should be done every Two years for High Risk customers, every Eight years for Medium Risk customers and every Ten years for Low Risk customers.	6	Banking services should not be denied to general public, especially, to those who are financially or socially disadvantaged.
7	Ensure that all the transactions where any forgery of a valuable security or a document has taken place facilitating the transactions are reported to Zonal Office within 3 days for submission by H.O. to Financial Intelligence Unit – India (FIU-IND), New Delhi.	7	In the accounts where a Suspicious Transaction Report (STR) has been made no restriction are put on the operations and it is ensured that there is no tipping off to the customers.
8	Demand Draft/Pay Order/mail transfer for Rs. 50,000/- and above is issued only by debit to customers account or against cheque and not against cash	8	Do not open new NRI accounts without a. Passport for verification with a copy. b. Work permit / permanent residency / Green Card etc. indicating the NRIs residential status abroad for verification with copy. c. NRI Declaration.
9	In case of all domestic inward remittances of Rs. 50,000/- and above and all foreign inward remittance of any amount, beneficiary account is credited only when complete originator information i.e. name, address and account number is available or after receipt of the originator information.		
10	Proper record of all transactions reported to ZO/HO in CCR and STR formats are maintained/ preserved for a period of at least 5 years from the date of cessation of each such transaction.		

ANNEXURE- II

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

No.	Suspicion	Summary of detection and review
1	False Identity	Identification documents were found to be forged during customer verification process. The account holder was not traceable.
2	Wrong Address	Welcome kit was received back as the person was not staying at the given address or address details given by the account holder were found to be false. The account holder was not traceable.
3	Doubt over the real beneficiary of the account	The customer not aware of transactions in the account. Transactions were inconsistent with customer's profile.
4	Account of persons under investigation	The customer was reported in media for being under investigation.
5	Account of wanted criminal	Name of the account holder and additional criteria (Date of birth/Father's name/Nationality) were same as a person on the watch list of UN, Interpol etc.
6	Account used for cyber crime	Complaints of cyber crime were received against a customer. No valid explanation for the transactions by account holder.
7	Account used for lottery fraud	Complaints were received against a bank account used for receiving money from the victims. Deposits at multiple locations followed by immediate cash withdrawals using ATMs. No valid explanation provided by the account holder.
8	Doubtful activity of a customer from high risk country	Cash deposited in a bank account at different cities on the same day. The account holder, a citizen of a high risk country with known cases of drug trafficking.
9	Doubtful investment in IPO.	Large number of accounts involving common introducer or authorised signatory. Accounts used for multiple investments in IPOs of various companies.
10	Unexplained transfers between multiple accounts.	Large number of related accounts with substantial inter-account transactions without any economic rationale.
11	Unexplained activity in dormant accounts	Sudden spurt in activity of dormant account. The customer could not provide satisfactory explanation for the transactions.
12	Unexplained activity in account inconsistent with the declared business	Transactions in account inconsistent with what would be expected from declared business. The customer could not provide satisfactory explanation.
13	Unexplained large value transactions inconsistent with client's apparent financial standing	Large value transactions in an account which usually has small value transactions. No valid explanation provided by the account holder.
14	Doubtful source of payment for credit card purchases	Credit card topped up by substantial cash first and then used for incurring expenses. Cumulative payment during the year was beyond known source of income.
15	Suspicious use of ATM card.	Frequent cash deposits in the account followed by ATM withdrawals at different locations. No valid explanation.
16	Doubtful use of safe deposit locker	Safe deposit locker operated frequently which is inconsistent with the financial status of client.
17	Doubtful source of cash deposited in bank account	Frequent cash transactions of value just under the reporting threshold. Cash transactions split across accounts to avoid reporting. No valid explanation provided.
18	Suspicious cash withdrawals from Bank account.	Large value cheques deposited followed by immediate cash withdrawals.
19	Doubtful source of foreign inward transfers in bank	Deposit of series of demand drafts purchased from Exchange House abroad. Sudden deposits in dormant account immediately followed by withdrawals.

No.	Suspicion	Summary of detection and review
	account	
20	Doubtful remitter of foreign remittances	Name and other details of the remitter matches with a person on watch list.
21	Doubtful beneficiary of foreign remittances	Name and other details of the beneficiary matches with a person on watch list.
22	Doubtful utilizations of foreign remittances	Foreign remittance being withdrawn in cash immediately. No valid explanation.
23	Misappropriation of funds	Reports of misappropriation of funds. Substantial cash withdrawals in account of a charitable organization.

ANNEXURE- III

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

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

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

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

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

@@@@@@@@@@