BANK OF INDIA

HEAD OFFICE

KYC / AML / CFT POLICY – 2019

Compliance Department

Head office

Index

Preamble

We have reviewed KYC/AML/CFT guidelines in view of amendments effected in Prevention of Money Laundering (PML) Act, RBI Master Direction-Know Your Customer (KYC) Direction, 2016 Feb 25, 2016 and updated on April 20, 2018, July 12, 2018 May 29, 2019 in line with Hon'ble Supreme Court Judgment in respect of Aadhaar Act on September 26, 2018 and GOI Gazette Notification dt.13.02.2019. This review be taken as an interim review as a revised Master Direction by RBI, Revision in Aadhaar Act and Amendment in PML Act is expected / awaited following Hon'ble Supreme Court Judgment on obtention of Aadhaar document / number for KYC purpose.

The reviewed policy covers KYC Standards and AML measures set through various gazette notifications of Government of India. Accordingly, it has been re-formulated / prepared by adopting ingredients contained in RBI Master Directions in respect of changes in set of Officially Valid Documents (OVDs) and defining Aadhaar which has now been embedded in the foundation of KYC framework.

Initially the KYC-AML policy document was formulated and adopted by our Bank as per Board approval dated 24.05.2005. Thereafter, the policy was reviewed from time to time by amending the guidelines issued by the regulators.

The policy expounds in detail the procedure towards Customer Due Diligence at the time of on-boarding of customer while establishing customer based relationship and subsequently during the course of operations in the account. It includes four key elements:

1) Customer Acceptance Procedure
2) Risk Management / Risk Categorization of Customers
3) Customer Identification Procedure, and
4) Monitoring of Transactions

The formulae under the policy shall provide continued guidance and safeguards to all our staff at various levels in Branches as well as in Administrative Offices for ensuring effective client relationship.

The policy defines Three Lines of Defense while implementing KYC-AML guidelines. These shall be helpful in strengthening the procedures at operational level and shall provide tools for ensuring enough robustness to the entire mechanism of KYC-AML-CFT Compliance at Bank level.

1. Objective

The objective of the Policy is:

To enable the Bank to know/understand the customers and their financial dealings better, thereby helping all concerns to manage KYC-AML-CFT related risks prudentially,

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

(b) To put in place a proper control mechanism for detecting and reporting of suspicious transactions in accordance with the statutory and regulatory provisions,

(c) To ensure that all the provisions of Prevention of Money Laundering Act, 2002 and the Rules made thereunder and all subsequent amendments thereto are duly complied with, and

(d) To ensure compliance with guidelines/instructions issued by the regulators, including FIU-IND and RBI.

2. Scope

Applicability,

a) RBI Master Direction-Know Your Customer (KYC) Direction, 2016 Feb 25, 2016 and updated on April 20, 2018, July 12, 2018 May 29, 2019 on adoption by our Bank, apply to our Bank being the entity regulated by RBI by granting us license under section 22 of Banking Regulation Act 1949.

b) These directions shall also apply to branches and majority owned subsidiaries of the Bank which are located abroad, to the extent they are not contradictory to the local laws in the host country, provided that:

i. Where applicable laws and regulations prohibit implementation of these guidelines, the same shall be brought to the notice of the Reserve Bank of India through Head Office, Compliance Department.

ii. In case there is a variance in KYC/AML standards prescribed by the Reserve Bank of India and the host country regulators, branches / subsidiaries should adopt the more stringent regulation of the two.

3. Definitions

As per RBI Master Directions, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

a) Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:

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

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

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

iv. **"Certified Copy of OVD"** - Obtaining a certified copy by regulated entity shall mean comparing the copy of officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the regulated entity.

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

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

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

vi. **CKYC** refers to Central **KYC** (**Know Your Customer**), an initiative of the Government of India. Thus, CKYCR will act as centralized repository of **KYC** records of investors in the financial sector with uniform **KYC** norms and inter-usability of the **KYC** records across the sector

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

a) the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,

Explanation - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.

viii. **e-KYC** or **eKYC** is a paperless Know Your Customer (KYC) authentication process, wherein the identity and address of the subscriber are verified electronically through Aadhaar authentication

ix. **"Non-profit organisations" (NPO)** means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.

x. **"Officially Valid Document" (OVD)** means

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

Provided that,

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

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

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

   ii. property or Municipal tax receipt;

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

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

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

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

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

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

xii. "Proof of possession of Aadhaar number"

No. 13012/184/2019/Legal/UIDAI (No. 2 of 2019).—Ministry of Finance (Department of Revenue) vide its Gazette notification dated 13.02.2019 has amended the Prevention of Money laundering (Maintenance of Records) Rules, 2005. These amendments inter alia include "proof of possession of Aadhaar number" in its list of officially valid document(s) provided under Rule 2(1)(d). As per the proviso to Rule 2(1)(d) whoever submits "proof of possession of Aadhaar number" as an officially valid document, has to do it in such a form as are issued by the Authority. In addition, a number of government departments and regulated entities also provide for Aadhaar as an officially valid document for identity verification of the resident.

Regulation 15 of the Aadhaar (Enrolment and Update) Regulations, 2016 ("Enrolment Regulations") which deals with delivery of Aadhaar number stipulates that, "Aadhaar number may be communicated to residents in physical form (including letters or cards) and/or electronic form (available for download through the Authority's website or through SMS)."

The Authority in exercise of the provisions under Regulation 35 of Enrolment Regulations hereby clarifies that delivery of Aadhaar number under Regulation 15 of the Enrolment Regulations means the issuance of Aadhaar number.

Further, the Authority in exercise of the provisions under Regulation 35 of the Enrolment Regulations hereby notifies that delivery of Aadhaar number under Regulation 15 shall mean and include the following:

a) **Aadhaar letter:** Issued by the Authority carries name, address, gender, photo and date of birth details of the Aadhaar number holder.

b) **Downloaded Aadhaar (e-Aadhaar):** Carries name, address, gender, photo and date of birth details of the Aadhaar number holder in similar form as in printed Aadhaar letter. This is digitally signed by the Authority as per Information Technology Act (Act No. 21 of 2000), which provides for legal recognition of electronic records with digital signature.

c) **Aadhaar Secure QR Code:** A quick response code generated by the Authority containing name, address, gender, photo and date of birth details of the Aadhaar number holder. This is digitally signed by the Authority as per Information

Technology Act (Act No. 21 of 2000), which provides for legal recognition of electronic records with digital signature.

d) **Aadhaar Paperless Offline e-KYC**: An XML document generated by the Authority containing name, address, gender, photo and date of birth details of the Aadhaar number holder. This is digitally signed by the Authority as per Information Technology Act (Act No. 21 of 2000), which provides for legal recognition of electronic records with digital signature.

The Aadhaar number holder can use any of the documents above to prove possession of Aadhaar number subject to the concerned entity's right to verify the genuineness of the above mentioned documents. The delivery of Aadhaar in any of its forms by itself may not be considered to be satisfactory proof of possession of Aadhaar number and the Aadhaar number holder may have to provide additional documents as may be required by the concerned entity.

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

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

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

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

a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
b) appears to be made in circumstances of unusual or unjustified complexity; or

c) appears to not have economic rationale or bona-fide purpose; or

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

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

xvi. A **'Small Account'** means a savings account which is opened in terms of sub-rule (5) of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are specified in Section 23.

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

a) opening of an account;

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

c) the use of a safety deposit box or any other form of safe deposit;

d) entering into any fiduciary relationship;

e) any payment made or received, in whole or in part, for any contractual or other legal obligation; or

f) Establishing or creating a legal person or legal arrangement.

b) Terms bearing meaning assigned in this Directions, unless the context otherwise requires, shall bear the meanings assigned to them below:

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

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

iii. **"Walk-in Customer"** means a person who does not have an account-based relationship with the Bank, but undertakes transactions with the Bank.

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

v. **"Customer identification"** means undertaking the process of CDD.

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

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

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

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

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

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

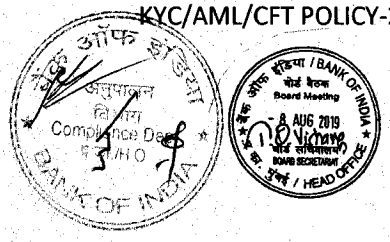
xi. **"Politically Exposed Persons" (PEPs)** are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important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

xii. **"Regulated Entities" (REs)** means

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

b) All India Financial Institutions (AIFIs)

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



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

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

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

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

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

c) All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder and 'Aadhaar and other Laws (amendment) Ordinance, 2019', any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

4. FINANCIAL INTELLIGENCE UNIT – INDIA

FIU-IND is a central agency; it is an independent body and reports directly to the Economic Intelligence Council headed by the Finance Minister.

(a) Its functions are to act as the central reception point for receiving CTR, STR, CCR, NPOTR and Cross Border Wire Transfer (CBWT) reports. It analyzes information received from banks to uncover pattern of transactions suggesting suspicion of money laundering and related crime.

(b) It disseminates the information to appropriate national / international authorities to support anti- money laundering efforts.

(c) It monitors and identifies strategic key areas on money laundering trends, typologies and developments.

(d) Director of FIU-IND is vested with the powers of a civil court under the code of Civil Procedure, 1908, accordingly has the power to seize, direct, penalize reporting entities and its employees for breach or violation of PML Act.

5. Obligations under Prevention of Money Laundering Act, 2002 (PML Act / Rules) include:

(a) Appointment of a Principal Officer (PO) and Designated Director (DD) (In no case, PO shall be designated as DD);

(b) Maintaining records of prescribed transactions;

(c) Furnishing information of prescribed transactions to the specified authority;

(d) Verifying and maintaining records of the identity of its clients and shall include updated records / data pertaining to identification, account files and business correspondence;

(e) Preserving records in respect of (b) and (c) above for a period of at least five years from the date of each such transaction between the Bank and the client;

(f) Preserving records in respect of (d) above for a period of at least five years after the business relationship is ended or the account is closed, whichever is later,

Principal Officer:

Bank is needed to appoint a senior management official as Principal Officer and he/she must be able to act independently and report directly to the senior management or to the Board of Directors and

- ✓ Should be located at the Head Office and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He / she shall maintain close liaison with the enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism,
- ✓ shall be responsible for overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002 and its amendments, rules and regulations made therein,

- ✓ shall be responsible for timely submission of Cash Transaction Report (CTR), Suspicious Transaction Report (STR), Counterfeit Currency Report (CCR), Non-Profit Organization Transaction Report (NPOTR) and Cross Border Wire Transfer (CBWT) report, to the FIU-IND,
- ✓ The staff working with him / her should have timely access to customer identification data and other customer due diligence information, transaction records and other relevant information for timely reporting to the regulators.

In our Bank, the General Manager in charge of Compliance Department has been appointed as the designated Principal Officer (Money Laundering Reporting Officer). The name, designation and address of the Principal Officer shall be communicated to the FIU-IND and RBI immediately after taking approval from the Board through HR.

Designated Director:

The bank is needed to designate a Director to ensure over all compliance of obligations imposed under PML Act and Rules. In our bank Executive Director has been appointed by the Board as Designated Director.

The HR Department shall ensure the appointment of the Designated Director as well as the Principal Officer and Compliance Department then shall communicate their respective name, designation and address to the FIU-IND.

The Provisions under Prevention of Money Laundering Act, 2002 (PML Act) and its amendments having taken place from time to time which are obligatory on every banking company, financial institution and intermediary.

The name, designation and address of the Designated Director shall be communicated to the FIU-IND and RBI immediately after taking approval from the Board through HR.

6. General

The KYC / AML / CFT policy shall be placed before the CORM for the clearance and then shall be placed before the Board for approval / adoption. The policy entails the procedure towards Basic Due Diligence / Customer Due Diligence / Enhanced Due Diligence while maintaining customer relationship and providing them various banking channels as per the requirements. It includes **four** major key elements-

(a) Customer Acceptance Procedure

(b) Risk Management / Categorization of Customer

(c) Customer Identification Procedure and

(d) Monitoring of Transactions.

The guidelines / directions under the policy shall provide continued guidance and safeguards to all our staff at various levels in Branches as well as in Administrative Offices during the course of client relationship and ensuring effective customer service.

The policy stipulates **Three Lines of Defence** while implementing KYC-AML guidelines; these shall be helpful in strengthening the procedures at operational level and shall provide tools for ensuring enough robustness to the entire mechanism at Bank level.

First Line of Defence: The policy shall provide the relevant guidelines and directions from regulators to front line staff at all our branches to deal with the customers at the time of on boarding and at subsequent stages.

Second Line of Defence: The administrative and supervisory lines in the branches and controlling offices shall provide necessary support and ensure putting necessary control mechanisms,

Third Line of Defence: The internal auditors conduct independent audit function to assess the compliance level to ensure effective compliance function in the Bank.

7. Implementation of Policy Guidelines and Compliance Monitoring:

Policy Formulation:- Compliance Department will ensure to formulate the policy in line with the guidelines issued by GOI, RBI and other related regulatory/statutory bodies. The policy shall be reviewed at annual interval. The department shall communicate, mostly by way branch circulars, to all concerns. If there happens any interim change in the regulatory

guidelines the department shall issue guidelines through Branch Circular/ Circular Letter and shall ensure to incorporate such change in the next version of the policy for review.

This policy is applicable to all branches of the bank and its banking/financial subsidiaries as well as the Depository Participant Offices of the Bank.

Branches will keep in mind that the process of account opening and establishing customer based relationship shall be strictly in accordance to this policy. The information collected for the purpose of opening of account will be kept as confidential and details thereof are not to be divulged for cross-selling or any other purposes.

Information sought from the customer should be relevant to the perceived risk as explained in detail further in this policy document and it should not be intrusive. Any other information from the customer should be sought separately with his/her consent only after opening of the account. Foreign Business Department should ensure that provisions of Foreign Contribution Regulation Act, 2010, wherever applicable, are strictly adhered to.

Policy Implementation:-The General Operation Department and all other functional departments depending on product related to their department shall implement the policy guidelines at field level. These departments shall ensure allocation of responsibilities for effective implementation of the policy and its procedures and shall also confirm compliances.

Compliance department through its Anti Money Laundering Cell shall put in place mechanism / procedure to monitor the compliances as prescribed by RBI and incorporated in this policy, given in brief, as under:

(a) Submission of Compliance in respect of KYC / AML / CFT rules in the form of templates on **monthly** basis by the branches to their Zonal Offices for onward submission to Head Office,
(b) Test check on half yearly basis by the officials from other branch / office,
(c) Procedure has been implemented to deploy Decoy Customers on yearly basis in selected branches on rotation basis,
(d) Internal / concurrent audit system to verify the compliance with KYC/AML policies and procedures,
(e) Submission of quarterly audit notes and compliance to the Audit Committee.

8. KYC Norms / Guidelines / Directions

Know your customer is the most important aspect in terms of legislative requirements. It refers to our relationship with customer at the time of on-boarding. Once customer based relationship is established it becomes resource for future customer banking relationship.

Knowing a customer is not just simply obtaining a copy of OVD. It is about the procuring knowledge and understanding about the normal life and business activity and practice of the customer to enable the Bank to recognize the clues/ signals which will indicate any suspicious activity related to the operations in the accounts at any stage.

In general terms, KYC is:

- Making every reasonable effort to determine the true identity and beneficial ownership of accounts
- Knowing the source of funds
- Knowing the correct location, address and nature of customer's business
- Knowing what constitutes reasonable account activity
- Knowing who are your CUSTOMERS' CUSTOMER

KYC norms, guidelines and directions for various banking activities have been enumerated in the policy in different para with details for meeting the compliance requirement at functionary level and ensuring effective implementation.

9. <u>Money Laundering:</u>

a) Definition:

As defined vide Section 3 of PML Act 2002 and further expanded (given vide Point 4.(c) above, it defines the "offence of money laundering" as under:

"Whosoever 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 crime <u>**including its concealment, possession, acquisition**</u> or use and projecting it as untainted property shall be guilty of the offence of money laundering".

In India AML activities are monitored by FIU-IND as per the provision of PML Act. Money laundering refers to any transaction that aims at concealing and/or changing the identity of criminal proceeds so that it appears to have been derived from legitimate sources.

b) **"Proceeds of Crime"** (as per section 2 of PML Act)

Means any property derived or obtained directly or indirectly by any person as a result of criminal activities. Money launderers use the banking system for cleansing 'dirty money' obtained from criminal activities with the objective of hiding/disguising its source.

c) The process of money laundering

It has been identified as being done generally in **three stages** and it involves creating a web of financial transactions so as to hide the origin and true nature of these funds. The three stages of money laundering are:

(i) 'Placement' (i.e. introduction of the funds into the banking system)

(ii) 'Layering' (i.e. creating a web of transactions and rotating the funds between various accounts so as to hide / extinguish its true source), and

(iii) 'Integration' (i.e. after rotating the funds, the money, now 'washed' appears to have legitimate source).

10. Risk Perception

Bank is exposed to the following risks which arise out of Money Laundering activities:

- **Reputation Risk:** Risk of loss due to severe impact on bank's reputation which is the most valuable asset of the organization;
- **Compliance Risk:** Risk of loss due to failure to comply with key regulations governing the Bank's operations;
- **Operational Risk:** Risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events;
- **Legal Risk:** Risk of loss due to any legal action, the Bank or its staff may face due to failure to comply with the law resulting in adverse judgments, unenforceable contracts, fines and penalties generating losses, increased expenses for an institution or even closure of such institution.

11. Customer Acceptance Policy (CAP)

In terms of RBI guidelines, the Customer Acceptance Policy (CAP) is one of four parameters which broadly define the KYC/AML/CFT guidelines. The CAP has been framed for ensuring compliance with all applicable regulatory guidelines while establishing customer relationship and maintaining the related accounts as per profile of the customers, the details as under:-

(a) No account shall be opened in anonymous / fictitious / benami name/s / shell companies.

(b) No accounts shall be opened where Bank is not able to apply CDD measures either due to non-cooperation of the customer or non-reliability of the KYC documents /information furnished by the customer / applicant.

(c) The mandatory information shall be sought for KYC purpose at the time of opening an account and during periodic updation. Any optional / additional information shall be obtained with the explicit consent of the customer after opening of the account.

(d) CDD procedure shall be applied at the Unique Customer Identification Code (UCIC) level. Accordingly, no fresh CDD exercise shall be required while opening another account by any existing customer in the Bank.

(e) CDD procedure shall be followed for all individuals including all joint account holders while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity:

(f) "Beneficial Owner" shall be identified / verified necessarily while opening / maintaining accounts having constitution as Partnership, Limited Companies, Trust etc. Details for compliance are given vide Point 15.

(g) Name screening of the prospective customer, before opening any account to be ensured that the identity of the prospective customer does not match with any person having known criminal background or with banned entities such as individual terrorists or terrorist organizations as advised by UN sanctions, OFAC, GOI, FIU-IND and RBI list being published from time to time. These lists have been made available through FINACLE on real time basis.

(h) Wherever accounts are opened and be operated by mandate holder or accounts are opened by intermediaries in fiduciary capacities, it should be ensured that the circumstances in which the said mandate holder or intermediary is permitted to act on behalf of another person/entity are clearly spelt out, in conformity with the established law and practice of banking.

(i) If the customer is a Politically Exposed Person (PEP) as per knowledge of the Bank, the account of such person will be approved by Branch Head before opening.

(j) Re-KYC exercise shall be carried out as per risk profile / category of the customers and Fresh set of KYC documents, latest Photograph & need based financials shall be obtained.

(k) No transaction or account based relationship is undertaken without following the CDD procedures.

(l) Information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or other purposes. It should be ensured that the information sought from the customers are relevant to the perceived risk, are not intrusive and are in conformity with the RBI guidelines issued in this regard.

While adopting / implementing all above guidelines / procedures, Bank shall ensure that banking / financial facility shall be made available with due care to the general public and specially those who are financially or socially disadvantaged.

12. Risk Management

In terms of RBI directions and PML Act 2002 requirements, a risk based approach has been adopted by the Bank for all type of customers to effectively address, manage and mitigate the risks.

(a) All customers new as well as existing are classified into risk categories i.e. Low, Medium and High based on the risk perception.

(b) Risk Based Approach has been designed based on profile of the customer i.e. customer's identity/occupation, the nature of business activity, information about the

client's business and their location, mode of payments, volume of turnover, social and financial status etc.

(c) The risk categorization is done initially based on the customer information submitted and verified as per the documents/ credentials at the stage of on–boarding of the customer. In order to enable the branches to classify correctly the customers' risk category, Compliance Department, HO has introduced a Customer Profile Sheet (CPS) which is required to be completed by the branch staff at the time of on-boarding of the customer / opening of the account / in case of need at the time of Re-KYC. Some of the indicative parameters for determining the risk category of a customer based on the profile of the customer are:

(i) Constitution: Individual, Proprietorship, Private/Public Ltd, Trust etc.
(ii) Business segment: Retail, Corporate, etc.
(iii) Country of residence/Nationality: India or any foreign country, Indian or foreign national,
(iv) Product subscription: Salaried, Business income, NRI products, etc.,
(v) Economic profile: High net worth individuals etc.
(vi) Account status: Active, Inoperative, and Dormant.
(vii) Volume of turnover, social and financial status, etc.
(viii) Politically Exposed Persons,
(ix) Geographical location within India (including the customer's clients)

(d) Branches shall prepare CPS for each new / if required for existing customer and assess / assign the risk category based on above mentioned parameters. The customer profile is a confidential document and details contained therein shall not be divulged either to the customer or for cross-selling / any other purposes. The nature and extent of due diligence will depend on the risk perceived by the bank.

(e) In terms of RBI guidelines, our Bank has classified certain category of occupations which are assessed as HIGH or MEDIUM since inception i.e. on-boarding of the customer to the running of such accounts throughout. The detailed list has been given vide **Annexure 1.**

(f) Customers who are likely to pose a higher than average risk to the Bank should be categorized as Medium or High Risk depending on the customers' background, nature

and location of activity, country of origin, sources of funds, client profile, etc. In such cases Enhanced /higher / intensive Due Diligence (EDD) shall be applied. Zones /branches should therefore apply Enhanced Due Diligence measures in case of higher risk customers, especially those for whom the sources of funds are not clear. The key components for due diligence are occupation, location, mode of payment, source of funds, volume and frequency of turnover etc.

(g) The accounts in which any kind of suspicion is observed or during the course of transaction monitoring and subsequent scrutiny the Suspicious Transaction Report (STR) is filed with FIU-INDIA, are categorized as HIGH mandatorily upon such finding / reporting.

(h) The risk categorization of customers shall be reviewed half yearly through a system driven procedure centrally in the Bank at Data Center level. Monitoring of transactions shall be one of the measure parameters for the Risk Based Approach. The process for half yearly review of risk categorization has been devised as under:

- The matrix have been prepared and put in the FINACLE system for risk categorization,
- Codes have been assigned for all type of occupations / activities and these have been uploaded into the Finacle system to identify / link the occupation / activity of the customer with the nature, value and volume of transactions as well as turnover in the account. Branches have been instructed to clearly specify / write occupation of the customer in the Account Opening Form and put the same in the system. Based on general perception and market study, occupation-wise threshold limits in respect of credit turnover in an account during twelve months have been put to standardize the risk matrix.
- All accounts are scanned under this matrix on half yearly basis i.e. September and March every year.

- Risk categories are re-assessed accordingly in the system and report is available at Branch end for applying Re-KYC norms / procedures in identified accounts, as under, depending on Risk Category:-

Risk Category	Re-KYC Period
LOW	Once in Ten Years
MEDIUM	Once in Eight years
HIGH	Once in Two Years

(i) Re-KYC shall be ensured in the accounts as per Risk category of the customer and as per stipulated frequency for which suitable notice shall be given to the customer advising to submit details as given vide Pt 16(f).

(j) The necessary emphasis has been given to make Risk Based Approach more effective. Steps in this regard have been initiated / put in place as under:

- ❖ Management oversight, systems and controls, have been ensured by way of monthly / quarterly reporting on KYC-AML Compliance,
- ❖ Specific responsibilities have been assigned to ensure that the policy and procedures are implemented,

13. Customer Identification Procedures (CIP)

(a) Bank shall undertake identification of customers in the following cases:

(i) Commencement of an account-based relationship with the customer.

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

(iii) When there is a doubt at any point of time about the authenticity or adequacy of the customer identification data obtained.

(iv) Selling third party products as agents, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.

(v) Carrying out transactions for a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

(vi) When the Bank has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.

(vii) Introduction is not to be sought while opening accounts.

(b) For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Bank shall not rely on third party for customer due diligence.

14. Customer Due Diligence (CDD)

A. Customer Due Diligence (CDD) Procedure in case of Individuals

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

a) a certified copy of any OVD containing details of his identity and address
b) one recent photograph
c) the Permanent Account Number (PAN) or Form No. 60 as defined in Income-tax Rules, 1962, and
d) Such other documents pertaining to the nature of business or financial status specified by the Bank in their KYC policy.

Provided that,

i. Banks shall obtain the Aadhaar number from an individual who is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016). Banks, at receipt of the Aadhaar number from the customer may carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India upon receipt of the customer's declaration that he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar

(Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 (18 of 2016) in his account.

ii. Banks may carry out Aadhaar authentication/ offline-verification of an individual who voluntarily uses his Aadhaar number for identification purpose.

iii. For non-DBT beneficiary customers, the Bank shall obtain a certified copy of any OVD containing details of his identity and address along with one recent photograph.

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

Provided further that in case biometric e-KYC authentication cannot be performed for an individual desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 owing to injury, illness or infirmity on account of old age or otherwise, and similar causes, Bank shall, apart from obtaining the Aadhaar number, perform identification preferably by carrying out offline verification or alternatively by obtaining the certified copy of any other OVD from the customer. CDD done in this manner shall invariably be carried out by an official of the Bank and such exception handling shall also be a part of the concurrent audit.

Bank shall ensure to duly record the cases of exception handling in a centralised exception database. The database shall contain the details of grounds of granting exception, customer details, name of the designated official authorising the exception and additional details, if any. The database shall be subjected to periodic internal audit/inspection by the Bank and shall be available for supervisory review.

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

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

Explanation 3: The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, the Aadhaar and Other Law (Amendment) Ordinance, 2019 and the regulations made thereunder.

Further:

a) **If there is change in name due to marriage**- for this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

b) In case the OVD furnished by the customer does not contain updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:-

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

(ii) property or Municipal tax receipt;

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

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

Provided further that the customer shall submit Aadhaar number voluntarily or provide OVD updated with current address within a period of **three** months of submitting the above documents."

c) The certified copy of the each OVD shall be obtained by comparing with original OVD so produced by the client and shall be recorded by writing **"Original seen and verified" by the authorized officer.**

d) In case the OVD submitted by a foreign national (Passport / National ID with identify and address) does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

e) **e-KYC:** Bank, at the time of receipt of the Aadhaar number submitted by the customer voluntarily, shall carry out, with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) or Yes/No authentication. The e-KYC service of Unique Identification Authority of India (UIDAI) shall be accepted as a valid process for KYC verification under the PML Rules, and

i. the information containing demographic details and photographs made available from UIDAI as a result of e-KYC process is treated as an 'Officially Valid Document', and

ii. Transfer of KYC data, electronically to the Bank from UIDAI, is accepted as valid process for KYC verification.

f) **Accounts opened using OTP based e-KYC, in non-face-to-face mode** are subject to the following conditions:

i. There must be a specific consent from the customer for authentication through OTP.

ii. The aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete.

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

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

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

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

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

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

g) **Small Account:** In case an individual customer who does not possess any of the OVDs and desires to open a bank account, banks shall open a **'Small Account'**, which entails the following limitations:

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

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

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

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

Further, **Small Accounts** are subject to the following conditions:

1. The bank shall obtain a self-attested photograph from the customer.
2. The designated officer of the bank certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

3. Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account.
4. Banks shall ensure that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place.
5. The account shall remain operational initially for a period of twelve months which can be extended for a further period of twelve months, provided the account holder applies and furnishes evidence of having applied for any of the OVDs during the first twelve months of the opening of the said account.
6. The entire relaxation provisions shall be reviewed after twenty four months.

7. The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, the identity of the customer shall be established through the production of an OVD and Permanent Account Number or Form No.60, as the case may be.
8. Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established through the production of an OVD and Permanent Account Number or Form No.60, as the case may be.

h) **KYC** verification once done by one branch/office of the Bank shall be valid for transfer of the account to any other branch/office in the Bank, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

i) **Walk-in Customers:** In case of transactions carried out by a non-account based customer, i.e. a walk-in customer, where the amount of transaction is **equal to or exceeds rupees fifty thousand**, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified and documentary proof of the same should be obtained and held on record. Wherever Bank has reason to believe that a walk-in customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50000/-, the Bank

should verify identity and address of such customer and also consider filing Suspicious Transaction Report (STR) to the Financial Intelligence Unit-India (FIU-IND).

Banks are required to verify the identity of the customers for all international money transfer operations.

B) CDD procedure for Proprietorship Accounts:

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

2) In addition to the above, any two of the following documents as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

   a) Registration certificate

   b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act.

   c) Sales and income tax returns.

   d) CST/VAT/ GST certificate (provisional/final).

   e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities.

   f) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.

   g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.

   h) Utility bills such as electricity, water, landline telephone bills, etc.

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

C) CDD Measures for Legal Entities

1. **In case of Company A/cs**

For opening an account of a company, certified copies of each of the following documents shall be obtained:

a) Certificate of incorporation

b) Memorandum and Articles of Association

c) Permanent Account Number (PAN) of the company

d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf

e) Documents, as specified in **Section 14-A**, of the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf (Authorised Signatory).

2. **In case of Partnership A/cs**

For opening an account of a partnership firm, the certified copies of each of the following documents shall be obtained:

a) Registration certificate

b) Partnership deed

c) Permanent Account Number (PAN) of the partnership firm

d) Documents, as specified in Section 14-A, of the person holding an attorney to transact on its behalf (Authorised Signatory).

3. **In case of Trust A/cs**

For opening an account of a trust, certified copies of each of the following documents shall be obtained:

a) Registration certificate

b) Trust deed

c) Permanent Account Number (PAN) or Form No.60 of the trust

d) Documents, as specified in Section 14-A, of the person holding an attorney to transact on its behalf (Authorised Signatory).

4. <u>In case of unincorporated association or a body of individuals A/cs</u>

For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents shall be obtained:

a) Resolution of the managing body of such association or body of individuals

b) Permanent Account Number (PAN) or Form No. 60 of the unincorporated association or a body of individuals

c) Power of attorney granted to transact on its behalf

d) Documents, as specified in Section 14-A, of the person holding an attorney to transact on its behalf (Authorised Signatory) and

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

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

Explanation: Term 'body of individuals' includes societies.

5. <u>In case of juridical persons A/cs</u>

For opening accounts of juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents shall be obtained:

a) Document showing name of the person authorised to act on behalf of the entity;

b) Documents, as specified in Section 14-A, of the person holding an attorney to transact on its behalf (Authorised Signatory) and

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

15. Beneficial Owner:

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

   a) Where the customer 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.

   b) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

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

   Explanation- For the purpose of this sub-clause-

   i. **"Controlling ownership interest"** means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.

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

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

4. Where the **customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

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

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

6. Where no natural person is identified, the beneficial owner is the relevant natural person who holds the position of senior management. Government of India has since examined the issue and has specified the procedure for determination of Beneficial Ownership.

7. A declaration from the legal entity duly certified by the statutory auditor of the legal entity shall be obtained for the purpose. The provision has been made in Finacle for entering the details of beneficial owner. A separate report has been provided in MISRPT (FINACLE) in this regard.

16. Ongoing Due Diligence and Monitoring of Transactions:

a) Once an account is opened and business relationship is established after ensuring KYC compliance, it is essential that the transactions in the account are monitored on an ongoing basis so as to achieve the ultimate objective of preventing the Bank from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.

b) Understanding of normal and reasonable activity of a customer enables the Bank to identify transactions that fall outside the regular pattern of activity. Transactions which **do not** fall within the ambit of the declared activity of the customer may be treated as suspicious and need to be reported to the FIU-IND. Special attention should be given to all complex, unusually large value transactions, transactions

involving large amount of cash inconsistent with the normal and expected activity of the customer, transactions having unusual patterns which have no apparent economic or visible lawful purpose, etc.

c) High risk category accounts should be subjected to intensive monitoring. Transactions in such accounts that involve large amounts of cash and / or non-cash inconsistent with the normal and declared business activity of the customer should essentially attract the attention of the bank. Very high turnover in account inconsistent with the size of the average balance being maintained, may indicate that funds are being 'washed' through the account.

d) Ongoing Monitoring shall be undertaken with guidelines to ensure that the transactions in the accounts are consistent with their knowledge about the customers, customers' business and risk profile; and the source of funds.

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

(i) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.

(ii) Transactions which exceed the thresholds prescribed for specific categories of accounts.

(iii) High account turnover inconsistent with the size of the balance maintained.

(iv) Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

e) The extent of monitoring shall be aligned with the risk category of the customer. Particularly intensified monitoring shall be undertaken in *High risk accounts,* with propositions as under:-

(i) A periodic review of risk categorization of accounts at least once in six months through system with matrix having parameters in respect of enhanced due diligence measures,

(ii) The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies to be monitored closely, i.e. cases where a large number of cheque books are sought by the company and/or multiple small

deposits (generally in cash) across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts/dates, shall be immediately reported to FIU-IND under STR.

f) Periodic updation of KYC (Re-KYC) as per stipulated frequency

Periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers as per the following procedure:

a) Re-KYC shall carry out as under:

i. CDD, as specified in **Section 14-A**, at the time of periodic updation. However, in case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.

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

iii. The customer profile sheet (CPS) shall be prepared afresh by the branch official keeping in view the review of risk assessment.

In case the customer dose not respond to the notice or does not submit the above details / documents, Branches shall temporarily cease operations (debit freeze) till the time any of required documents are not submitted by the customer, by giving an accessible notice as advised in Br. Circular / Circular Letter issued by the department from time to time and keeping proper records of such notices to the customers.

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

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

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

PAN requirement:

1. Accounts / Transactions in which PAN OR Form 60/61 required Rule 114B of the Income Tax Rules, 1962 has made it mandatory for the customer to quote the PAN for certain **banking** transactions, which have been detailed as below:

   (i) Placing a time deposit (i.e. a Term Deposit) EXCEEDING Rs.50,000/ with any Banking Company to whom the Banking Regulation Act, 1949 applies;

   (ii) Opening an account with a Banking Company to which the Banking Regulation Act, 1949 applies;

   (iii) Payment in cash for purchase of bank drafts or pay orders or banker's cheques FOR AN AMOUNT AGGREGATING TO RS. 50,000/- OR MORE DURING ANY ONE DAY, from a Banking Company to which the Banking Regulation Act, 1949 applies;

   (iv) A deposit in cash aggregating to Rs.50,000/- or more with a Banking Company to which the Banking Regulation Act, 1949 applies;

   (v) Making an application to any Banking Company to which the Banking Regulation Act, 1949 applies for issue of CREDIT OR DEBIT card;

2. In case the person making application for the transactions is a MINOR, who does not have any income chargeable to income tax, he / she shall quote the PAN of his / her father or mother or guardian, as the case may be.

3. **In case of existing customers**, Bank shall obtain the Permanent Account Number or Form No.60, by such date as may be notified by the Central Government, failing which Bank shall temporarily cease operations in the account till the time the Permanent Account Number or Form No. 60 is submitted by the customer.

   a) Provided that before temporarily ceasing operations for an account, the Bank shall give the client an accessible notice and a reasonable opportunity to be heard. Further, Bank shall include, in its internal policy, appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or Form No. 60 owing to injury, illness or infirmity

on account of old age or otherwise, and such like causes. Such accounts shall, however, be subject to enhanced monitoring.

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

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

17. Enhanced Due Diligence

(A) Accounts of NON –Face to Face customers:

Whenever any account is opened without visit of the customer to the Branch, e.g. NRI accounts, Branches should ensure that all the documents presented are certified to Bank's satisfaction, call for additional documents, if necessary. In such cases, as a prudent and precautionary measure, branches may also insist that the first credit be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards. In cases where certification is done by any third party, especially in case of cross border customers (where it is difficult to match the customer with the documentation), it must be ensured that the said third party is a regulated and supervised entity and has adequate KYC systems in place.

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

PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g. Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state owned corporations, important political party officials, etc. Sufficient information should be gathered on any person/customer

of this category intending to establish a relationship with the Bank and all the information available on the person in the public domain should be checked. Identity of such person/s should be verified and information about the sources of funds should be sought before accepting the PEP as a customer.

Bank shall have the option of establishing a relationship with PEPs provided that:

(a) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
(b) the identity of the person shall have been verified before accepting the PEP as a customer;
(c) the decision to open an account for a PEP is taken at a senior level in accordance with the Banks' Customer Acceptance Policy;
(d) all such accounts are subjected to enhanced monitoring on an on-going basis;
(e) in the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship;
(f) The CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable.

These above instructions will also be applicable to accounts where a PEP is the beneficial owner. The identification and EDD process must be very effective / meticulous in such cases.

(C) Clients' Accounts opened by Professional Intermediaries:

Bank will ensure while opening client accounts through professional intermediaries, that:

a) Clients shall be identified when client account is opened by a professional intermediary on behalf of a single client.

b) Bank shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.

c) Bank shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Bank.

d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of Bank, and there are 'sub-accounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of Bank, the Bank shall look for the beneficial owners.

e) Bank shall, at their discretion, rely on the 'customer due diligence' (CDD) done by an intermediary, provided that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.

f) **No account of any professional intermediaries on behalf of their client/s should be opened or held by the Bank where the professional intermediaries like lawyers, chartered accountants, etc., are unable to disclose the true identity of the owner of the account/funds due to any professional obligation of customer confidentiality.** Further no professional intermediary should be allowed to open any account on behalf of a client where Bank is not able to know and identify the client for any reason.

(D) Accounts of Non-Profit Organizations (NPOs):

An NPO is defined as:

"Any entity or organization that is registered as a Trust or a Society under the Societies Registration Act, 1860 (21 of 1860) or any State legislation or a Company registered under Section 8 of the Companies Act, 2013."

These accounts should be appropriately classified under appropriate Constitution Code in the Customer Master Maintenance menu of the Finacle system for effective monitoring / EDD.

18. Simplified Due Diligence:

(A) Simplified norms for Accounts of Self Help Groups (SHGs)

(a) CDD of all the members of SHG as per the CDD procedure mentioned in Section 14-A of this policy shall not be required while opening the savings bank account of the SHG.

(b) CDD as per the CDD procedure mentioned in Section 14-A of this policy of all the office bearers shall suffice.

(c) No separate CDD as per the CDD procedure mentioned in Section 14-A of this policy of the members or office bearers shall be necessary at the time of credit linking of SHGs.

At the time of opening account of SHG, KYC verification of all the members of SHG need not be done while opening the savings bank account of the SHG as KYC verification of all the office bearers would suffice.

As regards KYC verification at the time of credit linking of SHGs, it is clarified that since KYC would have already been verified while opening the savings bank account and the account continues to be in operation and is to be used for credit linkage, no separate KYC verification of the members or office bearers is necessary.

(B) Accounts of Foreign students studying in India.

(a) Bank shall, at its option, open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.

(i) Provided that a declaration about the local address shall be obtained within a period of 30 days of opening the account and the said local address is verified.

(ii) Provided further that pending the verification of address, the account shall be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of rupees fifty thousand on aggregate in the same, during the 30-day period.

(b) The account shall be treated as a normal NRO account, and shall be operated in terms of Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of FEMA. 1999.

(c) Students with Pakistani nationality shall require prior approval of the Reserve Bank for opening the account.

(C) Accounts of Non-Government Organizations (NGOs):

a) Accounts of NGOs should be opened only after fully complying with the KYC/AML/CFT guidelines. Accounts of NGOs receiving foreign contribution should be registered with the Ministry of Home Affairs, Government of India or possess prior approval of the Government for receiving foreign funds.

b) **All NGO accounts opened (except those promoted by the United Nations or its agencies) should be classified as High Risk category accounts AB INITIO and transactions in these accounts should be properly scrutinized with enhanced due diligence on continuous basis.**

c) All foreign inward remittances to the credit of these accounts should be scrutinized taking into account the customer profile, country of origin of funds, etc. and extant guidelines regarding such remittances.

(D) Simplified KYC norms for Foreign Portfolio Investors (FPIs):

Accounts of FPIs which are eligible/ registered as per SEBI guidelines, for the purpose of investment under Portfolio Investment Scheme (PIS), shall be opened by accepting KYC documents as detailed in Annex II, subject to Income Tax (FATCA/CRS) Rules.

Provided that banks shall obtain undertaking from FPIs or the Global Custodian acting on behalf of the FPI that as and when required, the exempted documents as detailed in Annex II will be submitted.

In terms of Rule 9 (14) (i) of the PML Rules, simplified norms have been prescribed for those FPIs who have been duly registered in accordance with SEBI guidelines and have undergone the required KYC due diligence/verification prescribed by SEBI through a Custodian/Intermediary regulated by SEBI. Such eligible / registered FPIs may approach a bank for opening a bank account for the purpose of investment under Portfolio Investment Scheme (PIS) for which KYC documents prescribed by the RBI would be required. For this purpose banks may rely on the KYC verification done by the third party (i.e. the Custodian/SEBI Regulated Intermediary) subject to the following conditions:

(i) the reporting entity immediately obtains necessary information of such client due diligence carried out by the third party;

(ii) the reporting entity 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;

(iii) the reporting entity 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;

(iv) the third party is not based in a country or jurisdiction assessed as high risk;

(v) the reporting entity is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable; and

(vi) Where a reporting entity relies on a third party that is part of the same financial group, the Regulator may issue guidelines to consider any relaxation in the conditions (1) to (4).

19. Maintenance and preservation of Records of Transactions/ Information:

A. Guidelines for Maintenance of Records of following Transactions:

- All transactions involving receipts by non-profit organizations, whether cash, clearing or transfer, of more than Rupees Ten Lakh or its equivalent, or its equivalent in foreign currency taken place within a month and all series of cash transactions which are integrally connected to each other having individual value in foreign currency in the accounts of Non-Profit Organizations,
- All cash transactions of the value of more than Rupees Ten Lakh below Rs.10 lakh or its equivalent in foreign currency, but the aggregate value exceeding Rs.10 lakh, taken place within a month,
- All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine,
- All transactions where any forgery of a valuable security or a document has taken place facilitating the transactions,
- All suspicious transactions whether or not made in cash, including attempted transactions,

- All transactions pertaining to Cross Border Wire Transfers of value more than Rs. 5 lacs or its equivalent in foreign currency.

B. Information to be preserved:

All necessary information in respect of transactions referred to above (a) should be preserved so as to permit reconstruction of individual transaction, including the following information:

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

C. Proper systems for Maintenance and Preservation of Records:

Branches should ensure that an appropriate system is in place for proper maintenance and preservation of records of transactions detailed hereinabove. The guidelines are enumerated below:

(i) The records should be maintained and preserved in a manner that allows the data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

(ii) As stated above, all necessary records of transactions, both domestic as well as 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, should be preserved for a **period of at least five years from the date of transaction between the bank and the customer.**

(iii) Records pertaining to the identification of the customer and his address (e.g. copies of KYC 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 a **period of at least five years after the business relationship has ended or the account is closed, whichever is customer**.

(iv) The identification records and transaction data should be made available to the competent authorities upon request.

(v) Record of all transactions reported in the Cash Transaction Report, Suspicious Transaction Report, Counterfeit Currency Report, Report of Non-Profit Organization(credits by cash or otherwise), Cross Border Wire Transfer (CBWT) , submitted to the FIU-IND should be preserved for a **period of at least five years from the date of transaction between the bank and the client.**

(vi) Specific guidelines have been issued to the Internal Auditors / Concurrent Auditors for carrying out audit of adherence to KYC/AML/CFT guidelines during audit of the Branches.

Note: Maintenance and preservation of Records of Transactions/ Preservation of Information shall be the responsibility of each department in administrative offices depending on the respective area of works and branches.

20. Reporting

Reporting to Financial Intelligence Unit – India:

In terms of the PML Act Rules following Reports are to be submitted to the Financial Intelligence Unit-India (FIU-IND), Ministry of Finance, Government of India, New Delhi:

(a) Cash Transaction Report (CTR): (Frequency- Monthly)

CTR for every month is to be submitted by 15th of the succeeding month and shall include:

(i) All cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency taken place within a month.

(ii) All series of cash transactions integrally connected to each other (aggregate value of all debit OR all credit transactions, irrespective of value of each transaction), where series of such transactions have taken place within a month and aggregate value of all such transactions exceeds Rupees Ten Lakh or its equivalent in foreign currency.

(iii) **Anti-Money Laundering Cell, HO** shall generate CTR through AMLOCK where the transaction data in Finacle is uploaded. The report is generated in form of XML file and the same gets converted and validated to a # file through the report validity utility of FIUIND.

(iv) On submission of CTR to FIU-IND, all the transactions captured in the Report shall be segregated Zone wise / Branch wise and sent to the respective Zones for onward

transmission to the respective Branches. The Branches shall scrutinize the transactions and confirm to their Zonal Office that the transactions are genuine and in line with the business/activity of the customer and confirm that no money laundering is involved. Zonal Offices, in turn, submit consolidated certificate to Head Office. Transactions found to be suspicious in nature are reported by the Branch / Zonal Office to Anti Money Launder Cell, Compliance Department, HO for reporting under STR.

(v) Record of all transactions reported in the Cash Transaction Report will be preserved for a **period of at least five years from the date of transaction between the bank and the client.**

(b) SUSPICIOUS TRANSACTION REPORT (STR): (Frequency- as and when noticed)

(i) Suspicious Transaction Reports (STRs) in respect of accounts / persons are submitted to the FIU-IND as and when Red Flag Indicators (RFIs) are identified as defined vide various alerts prescribed by FIU / IBA.

(ii) An Anti-Money Laundering Package called AMLOCK has been installed in Compliance Department, Head Office for getting alerts pertaining to RFIs and to identify suspicious transactions. Various scenarios as per these RFIs prescribed by FIU /IBA have been configured in the package. Financial parameters have been assigned to each of the scenarios/RFIs. After End of Day operations (EOD) in the Finacle system, the entire transaction (data) is uploaded in the AMLOCK (daily basis). The AMLOCK processes the data on the basis of the scenarios available and generate the alerts matching the transactions visa-a-visa scenarios.

(iii) These Alerts, so generated through AMLOCK, are scrutinized with money laundering aspect and to ascertain whether the transactions are indeed of suspicious nature, being not in tune with the business / activity of the relative customer and/ or without any economic rationale etc.

(iv) The AMLRO (Anti money laundering reporting officers) in AML cell, Compliance Department, HO scrutinize the alerts apart from seeking information from the branches and present such cases to a **Screening Committee** Headed by DGM or AGM and two Chief Managers from Compliance Department, one officer of the rank of Chief Manager / Senior Manager from Fraud Risk Management Department or General Operation Department to approve the scrutinized cases for filing of STR as

per merit of each case. The STR has to be reported to FIU IND within 7 days from the date decision is taken by the screening committee,

(v) There are several other indicators of non-financial nature which could give rise to an equal amount of suspicious and result in filing STR; these offline alert scenarios are as per **Annexure 2** attached.

(vi) It is likely that in some cases transactions are abandoned / aborted by customers on being asked to give some details or to provide documents. It is clarified that all such attempted transactions should be reported as STRs, even if not completed by customers, irrespective of the amount of the transaction.

(vii) STRs should be reported if there is a reasonable ground to believe that the transaction involves proceeds of crime generally, irrespective of the amount of transaction.

(viii) The Zones / Branches should ensure that the customers are **NOT TIPPED OFF** in any manner whatsoever regarding our enquiry. Scrutiny of the transactions and enhanced due diligence should be done in completely discreet manner.

(ix) Branches Zones, wherever, find any suspicion in respect of financial or non-financial transactions / attributes of a customer, may report the matter to Compliance Department, Head Office for filing of STR. Submission of STR in an account should in **no way restrict operations** in that account and the customer **should not be aware** about such action i.e. STR has been filed in the account.

(x) Record of all transactions reported in the Suspicious Transaction Report should be preserved for a **period of at least five years from the date of transaction between the bank and the client.**

(c) Counterfeit Currency Report (CCR): (Frequency- Monthly)

(i) All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported by the Principal Officer of the bank to FIU-IND in the specified format(Counterfeit Currency Report - CCR), by 15thday of the next month. These cash transactions should also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

(ii) Once a counterfeit currency transaction is detected, the same should be reported by the Branch to the respective Zonal Office in the prescribed CCR format immediately and in any case **within two days** from the date of such detection. Zonal Office should

scrutinize the same and submit their CCR in the prescribed format duly signed by the concerned Zonal Manager / Nodal Bank Officer (as per RBI- all cases of reporting of counterfeit note detection should be through the Nodal Bank Officer) **within two days from the date of submission by the Branch** to the Compliance Department, Head Office to enable the Principal Officer at Head Office to submit the CCR to the FIU-IND within the mandatory time limit of 15th of the following month.

(iii) **Compliance Department,** HO shall generate CCR through AMLOCK where the transaction data in Finacle is uploaded.

(iv) RBI has relaxed the rules in respect of filing of FIR i.e. for up to 4 (four) counterfeit currency notes per transaction **FIR need not be filed**. Instead, a consolidated monthly statement is to be sent to the police authorities, enclosing therewith the counterfeit currency notes. In respect of counterfeit currency notes of 5 (five) and above, FIR has to be filed along with counterfeit notes. **Under no circumstances the counterfeit currency notes are to be returned to Customers**. As per the implementation of Reserve Bank of India Clean note policy, detection, impounding and reporting of counterfeit notes are revised. Branches are advised to accept all forged notes of customer and credit the full value to his account. All Zones / Branches / Offices are advised to refer circular letter No 2013-14/155 ref GOD/DDK/13/14 dated 18.11.2013 / RBI circular No.DCM(FNVD)G-4/16.01.05/2017-18 DT.20.07.2017 in this regard.

Record of all transactions reported in the Counterfeit Currency Report should be preserved for a **period of at least five years from the date of transaction between the bank and the client.**

(d) Non-Profit Organization Transactions Report (NPOTR): (frequency-monthly)

(i) All transactions involving receipts of value more than Rupees Ten Lakh or its equivalent in foreign currency by Non-Profit Organizations should be submitted every month to the FIU-IND by the 15th of the succeeding month in the prescribed format by the Principal Officer.

(ii) HO shall generate NPOTR through AMLOCK where the transaction data in Finacle is uploaded.

(iii) Record of all transactions reported in the Non-Profit Organization Report should be preserved for a **period of at least five years from the date of transaction between the bank and the client. Compliance Department.**

(e) Cross Border Wire Transfers Report (CBWTR): (Frequency- Monthly)

All Cross Border Wire Transfers whether originated in India or destination is India, above Rupees Five lacs or its equivalent in foreign currency has to be reported every month (by the 15th of the succeeding month) to FIU-IND as per the recent amendment to PML Act 2002. **Compliance Department,** HO shall generate CBWTR through AMLOCK where the transaction data in Finacle is uploaded.

Note: All the above reports are generated in form of XML file and the same gets converted and validated to a # file through the report validity utility provided by FIU-IND. The validated file is then uploaded to FIU-IND site under the digital signature of the Principal Officer.

21. Requirements / obligations under International agreements Communications from International Agencies-

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

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

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

(c) Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated August 27, 2009.

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

(e) Banks is required to check names / credentials of account holder, new as well as existing, to ensure that ~~as~~ these do not appear in the list of terrorist individuals /organizations banned by the United Nations' Security Council Sanctions Committee as circulated by the RBI from time to time.

22. Freezing of Assets under section 51 A of Unlawful Activities Act, 1957

The procedure laid down in the UAPA Order dated August 27, 2009 (Annex I of RBI Master Direction shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The Government Order on Procedure for Implementation of Section 51A of The Unlawful Activities (Prevention) Act, 1967 is given in **Annexure-4.**

23. Jurisdictions that do not or insufficiently apply the FATF Recommendations

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

b. Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

Explanation: The process referred to in Section 55 a & b do not preclude Banks from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.

c. The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and

written findings together with all documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.

24. Secrecy Obligations and Sharing of Information:

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

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

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

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

(i) Where there is a duty to the public to disclose,

(ii) The interest of bank requires disclosure and

(iii) Where the disclosure is made with the express or implied consent of the customer.

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

(a) Bank shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the revised KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015.

(b) The 'live run' of the CKYCR should start with effect from July 15, 2016 in phased manner beginning with new 'individual accounts'. Accordingly, Bank shall take the following steps:

(i) Bank shall invariably upload the KYC data pertaining to all new individual accounts opened on or after January 1, 2017 with CERSAI in terms of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005. However,

time has been allowed up to February 1, 2017 for uploading date in respect of accounts opened during January 2017.

(ii) Operational Guidelines (version 1.1) for uploading the KYC data have been released by CERSAI. Further, 'Test Environment' has also been made available by CERSAI for the use of Banks.

26. Foreign Account Tax Compliance Act (FATCA) & Common Reporting Standard (CRS)

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

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

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

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

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

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

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

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

i. updated Guidance Note on FATCA and CRS

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

In our Bank, the Executive Director and General Manager in charge of GOD have been appointed as the designated Director and Principal Officer (FATCA and CRS) respectively. The General Manager, GOD shall ensure implementation of FATCA – CRS and its reporting obligations.

A note on FATCA /CRS compliance and Reporting is given vide **Annexure-3**

27. Period for presenting payment instruments

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

28. Collection of Account Payee Cheques

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

29. Operation of Bank Accounts & Money Mules:

The instructions on opening of accounts and monitoring of transactions shall be strictly adhered to, in order to minimise the operations of "Money Mules" which are 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 which act as "money mules." If it is established that an account opened and operated is that of a Money Mule, it shall be deemed that the bank has not complied with these directions.

The accounts, if identified at any point of time appear to be of "Money Mules", must be monitored closely and must be advised to Anti Money Laundering Cell, HO for stating the reason of suspicion. In such cases Suspicious Transaction Report (STR) must be filed and Branches must undertake Re-KYC exercise.

30. Credit / Debit / Smart / Gift Cards, Mobile Wallet, Net Banking/ Mobile Banking, RTGS/ NEFT/ ECS/ IMPS, Demat Services/ E-KYC- Money Laundering Threats from new technology

Adequate attention shall be paid by Banks to any money-laundering and financing of terrorism threats that may arise from new or developing technologies and it shall be ensured that appropriate KYC procedures issued from time to time are duly applied before introducing new products/services/technologies. Agents used for marketing of credit cards shall also be subjected to due diligence and KYC measures.

(a) **Cards Business:**

Our Bank is in the business of issuing various types of cards that are used by customers for buying goods and services, drawing cash from ATMs and can also be used for electronic transfer of funds. Credit cards include issuance of Branch Billing Cards as well as Direct Billing Cards. In case of Branch Billing Cards, the customers are required to maintain account with the Branch which is considered as charge account for debiting the bills. Branches should ensure that KYC norms are fully complied with before issuance of cards to the Branch customers.

In respect of Direct Billing Cards, as the persons to whom these cards are issued are non-customers Branches should importantly note to carry out extensive customer due diligence before issuance of cards to them. Complete KYC exercise should be done. Apart from obtaining recent photograph, proof of identity and address from such non-customers, Branches should ensure proper verification of the documents submitted to them so as to confirm authenticity of the documents.

Branches are also required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on card-holders.

The Card Product Department, HO shall ensure that required KYC compliance and proper due diligence measures are being taken by the Branches before an acquirer is issued with any card product.

(b) **Money laundering threats from new technologies:**

Branches should pay special attention to any money laundering threats that may arise from new or developing technologies like internet banking, mobile banking etc. that might favour anonymity and take measures, if needed, to prevent their use in money-laundering schemes. Branches should extend such facilities only to those accounts that are fully KYC compliant, as per extant KYC/AML/CFT guidelines.

The Alternative Delivery Channel Department, HO shall ensure that required KYC compliance and proper due diligence measures are being taken by the Branches before providing any IT enabled product like internet banking / mobile banking etc.

(c) **Depository Services:**

Our bank is extending Depository services to the customers. The services are rendered through two Depository Participant Offices viz. Central Depository Services Ltd. (CDSL) and National Securities Depository Ltd. (NSDL).

As per the existing business model, Demat Accounts are opened only of those customers who have a duly KYC compliant Banking Account with our Bank or for one who opens a KYC compliant Banking Account with our Bank. Branches should importantly note that Demat accounts should be recommended by them only in respect of their KYC compliant customers. Moreover, the Branch/Office forwarding the Demat Account Opening Form (AOF) of a prospective customer is required to ensure proper identification/verification and follow the guidelines issued by our Bank/Depositories/Regulatory Authorities.

All the guidelines applicable for a Banking Account are applicable to Demat Account also and therefore, it should be ensured by the Branches/Offices that Due Diligence in respect of Banking Account of Demat customer is carried out.

31. Wire Transfers

Bank shall ensure the following while effecting wire transfer:

a) All cross-border wire transfers including transactions using credit or debit card shall be accompanied by accurate and meaningful originator information such as name, address and account number or a unique reference number, as prevalent in the country concerned in the absence of account.

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

b) Domestic wire transfers of rupees fifty thousand and above shall be accompanied by originator information such as name, address and account number.

c) Customer Identification shall be made if a customer is intentionally structuring wire transfer below rupees fifty thousand to avoid reporting or monitoring. In case of non-cooperation from the customer, efforts shall be made to establish his identity and STR shall be made to FIU -IND.

d) Complete originator information relating to qualifying wire transfers shall be preserved at least for a period of five years by the ordering bank.

e) A bank processing as an intermediary element of a chain of wire transfers shall ensure that all originator information accompanying a wire transfer is retained with the transfer.

f) The receiving intermediary bank shall transfer full originator information accompanying a cross-border wire transfer and preserve the same for at least
five years if the same cannot be sent with a related domestic wire transfer, due to technical limitations.

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

h) Effective risk-based procedures to identify wire transfers lacking complete originator information shall be in place at a beneficiary bank.

i) Beneficiary bank shall report transaction lacking complete originator information to FIU -IND as a suspicious transaction.

j) The beneficiary bank shall seek detailed information of the fund remitter with the ordering bank and if the ordering bank fails to furnish information on the remitter, the beneficiary shall consider restricting or terminating its business relationship with the ordering bank.

32. Issue and Payment of Demand Drafts, etc.,

Any remittance of funds by way of demand draft, mail/telegraphic transfer/NEFT/IMPS or any other mode and issue of travelers' cheques for value of rupees fifty thousand and above shall be effected by debit to the customer's account or against cheques and not against cash payment.

Further, the name of the purchaser shall be incorporated on the face of the demand draft, pay order, banker's cheque, etc., by the issuing bank. These instructions shall take effect for such instruments issued on or after September 15, 2018.

33. Correspondent Banking:

Banks shall have a policy approved by their Boards, or by a committee headed by the Chairman/CEO/MD to lay down parameters for approving correspondent banking relationships subject to the following conditions:

a. Sufficient information in relation to the nature of business of the bank including information on management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the bank's home country shall be gathered.
b. Post facto approval of the Board at its next meeting shall be obtained for the proposals approved by the Committee.
c. The responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented.
d. In the case of payable-through-accounts, the correspondent bank shall be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking on-going 'due diligence' on them.
e. The correspondent bank shall ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

f. Correspondent relationship shall not be entered into with a shell bank.

g. It shall be ensured that the correspondent banks do not permit their accounts to be used by shell banks.

h. Banks shall be cautious with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.

i. Banks shall ensure that respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

Bank's 'Correspondent Banking' policy in this regard was approved at the Board Meeting held on 18.04.2017. (International Division's Memorandum No. INTL (FBD) MDG: 16-17:62 dated 20-02-2017).

34. Name Screening against Sanctioned / Banned lists including OFAC & Politically Exposed Person (PEP) list

As per mandate/guidelines of RBI, new functionality has been introduced for online screening of customer names and related available details with following lists, at the time of verification of customer ID.

(a) United Nations List:-The Consolidated Sanctions List includes all individuals and entities subject to sanctions measures imposed by the Security Council.

(b) OFAC with Accuity Enhancements:-

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against

- targeted foreign countries and regimes,
- terrorists,
- international narcotics traffickers,
- those engaged in activities related to the proliferation of weapons of mass destruction, and

- other threats to the national security, foreign policy or economy of the United States

As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries and individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs."https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_lists.aspx

(i) Indian Ministry of Home Affairs List

(ii) India National Investigation Agency List

(iii) PEP Database - Global List

Branches / Offices are advised to refer circular letter No 110/100 dated 07.09.2018 issued by Compliance Department, HO in respect of name screening at the time of onboarding. Similarly, Branches / Offices are advised to refer circular letter No INTL/FBD/TSN/14-15:30 dt.24.02.2015 issued by Foreign Business Department, HO in the matter specifically in relation to foreign remittances for name screening while effecting foreign remittances by AD Branches.

35. Selling third party products

Bank acting as agents while selling third party products as per regulations in force from time to time shall comply with the following aspects for the purpose of these directions:

(a) the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under Section 13(e) of this Directions.

(b) transaction details of sale of third party products and related records shall be maintained as prescribed in Chapter VII Section 46.

(c) AML software capable of capturing, generating and analysing alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.

(d) transactions involving rupees fifty thousand and above shall be undertaken only by:

- debit to customers' account or against cheques; and

- obtaining and verifying the PAN given by the account based as well as walk-in customers.

(ii) Instruction at 'd' above shall also apply to sale of Bank's own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.

36. At-par cheque facility availed by co-operative banks

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

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

(c) Cooperative Banks shall:

I. ensure that the 'at par' cheque facility is utilised only:

a. for their own use,

b. for their account-holders who are KYC complaint, provided that all transactions of rupees fifty thousand or more are strictly by debit to the customers' accounts,

c. for walk-in customers against cash for less than rupees fifty thousand per individual.

II. maintain the following:

a. records pertaining to issuance of 'at par' cheques covering, inter alia, applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheque,

b. Sufficient balances/drawing arrangements with the commercial bank extending such facility for purpose of honouring such instruments.

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

37. Issuance of Prepaid Payment Instruments (PPIs):

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

38. Operational Procedure:

KYC –AML-CFT norms, guidelines and directions for various banking activities / products have been enumerated in this policy in different para with details for meeting compliance requirement by the functionaries at operational level. In reference to these policy guidelines, the functional departments at HO as per an indicative list given as under, shall therefore prepare and disseminate detailed operational procedures to the Branches for effective implementation of KYC-AML-CFT compliance and ensure its monitoring.

Name of Activity / Product	**Functionary Level / Operational Departments**
Customer acquisition- Opening & maintaining deposit accounts, FATCA & CRS	General Operations Department (GOD) /Centralised Back Office Department (CBOD)
Customer acquisition- Opening & maintaining advances accounts	Credit Department (C&IC , SME, Retail & AFD) ,
Correspondent Banking	FBD
Credit Card / Debit Cards	Card Product Department / Alternate Delivery Channel
Remittances	GOD, HO (Domestic Remittances) and the Foreign Business Department, HO for CBWT.
Third party products	Marketing Department
Maintenance and Preservation of Records	Responsibility of each department in administrative offices depending on the respective area of works and branches.
Appointment of venders , Advocates , Valuers, etc	Respective departments engaging such people / agencies.

	Example- Financial Inclusion Department for appointment of BCs / BFs
Information Technology and information security.	Information Technology & Information Security

39. Effective implementation, control and reporting is ensured by the following measures:

Compliance Department, HO undertakes compliance monitoring to ensure compliances using following tools and reports to Board / Top Management regarding compliance status periodically.

- Monthly confirmation to KYC-AML-CFT compliance rules (CR-12) by Branches /Zones and verification of same by internal auditors. Compliance Department, HO has prepared a compendium of KYC/AML/CFT guidelines incorporating up to date guidelines in CR-12 format and circulated to all the Zones/Branches.
- This is a comprehensive certificate in the form of templates required to be submitted by the Branches every month to their respective Zonal Office, certifying compliance of KYC-AML-CFT guidelines.
- Zones, in turn, are required to send their consolidated certificate to the Compliance Department, HO every month.
- Conduct of Compliance testing at branches on half-yearly basis in India and quarterly for overseas branches
- Use of decoy customer exercise in respect of KYC-AML-CFT compliance on annual basis at branches in India
- Inspection & Audit:

Risk based Internal Audit and Concurrent Audit shall check and verify the application of KYC procedure at the branches and comment on the lapses observed in this regard. The compliances in this regard are put up before the Audit Committee of the Board on a quarterly basis.

40. KYC-AML COMPLIANCE AT FOREIGN CENTERS

The center specific policy in respect of various products / work areas, compliance standards to meet KYC/AML/CFT measures being the primary requirement, its formulation will consider adoption of various applicable laws / rules/regulations / industry level best practices, stringent of host country and home country, for different products or services rendered by the bank at the center. The Chief Executive / Branch Head of the center / Branch will identify / authorize officer(s) in the Branch / Center to formulate / undertake drafting of center specific KYC/AML/CFT policy for annual review taking into account all these aspects.

(a) The Chief Executive at each overseas center is responsible for implementation of the KYC-AML-CFT compliance function in the concerned center / territory. A compliance officer (CO) shall be posted at each overseas establishment. Preferably a local officer having knowledge of compliance functions as well conversant with local laws and also acceptable to Local Regulators shall be recruited / posted for the purpose. However, India Based Officers may also be assigned such responsibilities as per consent of Local regulators. CO will be the responsible to ensure compliance of rules / regulations / norms on KYC-AML-CFT. CO shall acquire knowledge of related statutory and regulatory guidelines prevailing in the territory / other countries and also bank's internal guidelines, general or specific for the center/ branch.

(b) Before the policy being approved for adoption and implementation, The Chief Executive at the center will further ensure to put in place a system for scrutiny / review of the KYC/AML/CFT policy locally in Branch / Center level compliance committee / risk management committee having the compliance officer and/or concurrent auditor as member(s).

(c) Further, in order to meet the challenges of dynamisms in global regulatory frameworks, ensuring coverage of all KYC-AML-CFT requirements in the policy, the Chief Executive of the center will ensure vetting of the policy through a locally reputed professional firm at the time of formulation of the new policy or at least once on each alternate year for annual review. The Branch will have to obtain a certificate of confirmation from the professional firm in effect of vetting of the policy and confirming above requirement. However, in case of review, where there will be no major

regulatory changes or regulatory examination / audit recommendations during the review year, such vetting may be waived by The Chief Executive with proper noting.

(d) The Compliance Officer (CO) will monitor implementation of the KYC-AML-CFT policy in the branch / center and report the findings while submitting periodical compliance reports to the General Manager & Chief Compliance Officer (GM & CCO), Head Office independently with whom CO shall be responsible to maintain a dotted line reporting. As a part of this exercise, he /she will also ensure to include KYC-AML-CFT issues in his/her overall compliance testing to be undertaken periodically preferably at quarterly intervals.

41. Customer Education/Employee's training/Hiring of Employees:

(a) Customer Education:

Implementation of KYC procedures requires us to demand certain information from the customers which may be of personal nature or which have hitherto never been called for. This can sometimes lead to questioning by the customers as to the motive and purpose of collecting such information. It is, therefore, necessary to prepare specific literature/pamphlets etc. so as to educate the customers of the objectives of the KYC programme. Necessary guidelines in this regard are issued by Compliance Department, KYC/AML cell from time to time.

(b) Employee Training:

Bank has planned to arrange at least 1/2 sessions on KYC /AML measures mandatorily in each training programme being conducted in all our Staff Training Colleges so that the staff members are adequately trained in these area of concern. The training guides the staff to understand fully the rationale behind the KYC/AML/CFT policies and implement the same consistently. The Staff Training Colleges have been instructed to ensure compliance in the matter.

Full day workshops are organized at Zonal Offices / NBG offices to sensitize staff members.

E- Learning modules through HRMS have been prepared / introduced for increasing awareness level

A small booklet namely "Guidance Notes for Staff" in respect of KYC / AML/ CFT has been prepared by Compliance Department, Head Office and circulated amongst all staff to increase the awareness level of on the subject as well as act as a Ready Reckoner.

(c) Hiring of Employees:

KYC/AML/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking channels. It is, therefore, necessary that adequate screening mechanism is put in place by the Bank as an integral part of the recruitment/hiring process of personnel. Necessary inputs in this regard have been incorporated in Bank's HR Policy.