
# BOMBAY MERCANTILE CO-OPERATIVE BANK LTD.

**(SCHEDULED BANK)**

# Anti Money Laundering & KYC Policy

2019-2022

**Regd. Office :**
78, Mohammedali Road, Mumbai - 400 003.
Tel. : 022 2342 5961 (4 Lines)

**BOMBAY MERCANTILE**
**CO-OPERATIVE BANK LTD.**
**(SCHEDULED BANK)**

Phone : 2342 5961(4 lines) / Fax : +91-22-2343 003
Visit us at : www.bmcbankltd.com
89, Mohamedali Road, Mumbai - 400 003
Grams : "KHAZANCHI" Chinchbunder, Mumbai 400 009. Telex : 011-73727 BMCB II

Ref. No. 81/AGM/KYC/2019-2022

Date : 08.03.2019

# Anti-Money Laundering Policy

**Policy On Know Your Customer (KYC) and Anti Money Laundering Measurers from 1st April 2019 to 31st March 2022**

The Board in their meeting held on 08.3.2019, has approved this policy of the bank on 'Know Your Customer (KYC) and Anti Money Laundering Measurers' for implementation by the Bank. We enclosed herewith the copy of this policy along with the modalities to be followed by the staff at supervisory and functional level. This policy represents the basic standards of the requirement of the Anti-Money laundering and Combating Terrorism Financing (hereinafter collectively referred to as AML) procedures within the Bombay Mercantile Cooperative Bank Ltd. All Branch Managers are advised to circulate this instruction to the Officers / Staff of the bank and to study the instruction contained therein. As you are aware that the KYC Policy of the bank was approved by the Board on 14.8.2016. There has been modification / changes by RBI in the KYC requirements of the Bank in terms of their Master direction updated July 2018 and subsequent changes if any, issued by RBI from time to time.

It is therefore become necessary to incorporate the changes as per the directions of RBI. Branches are therefore advised to ensure strict adherence to the KYC/AML guidelines as per the policy of the bank and all other instruction issued by RBI from time to time.

MOHAMED ARIF AMIRI
PRINCIPAL OFFICER

**BOMBAY MERCANTILE COOPERATIVE BANK LTD.**
**SCHEDULED BANK.**

# ANTI MONEY LAUNDERING & KNOW YOUR CUSTOMER POLICY OF YEAR 2019 – 2022.

**The Policy on KYC standards and AML measures**

## PREAMBLE

## GENERAL

The Prevention of Money Laundering Act, 2002 (PMLA) brought into force with effect from 1st July, 2005, is applicable to all the Reporting Entities (RE) as defined in the said Act. Section 12 of the PMLA places certain obligations on the reporting entities which are as follows:

a. Maintain a record of all transactions, including information relating to transactions covered under clause (b), in such manner as to enable it to reconstruct individual transactions;
b. Furnish to Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value as may be prescribed.
c. Verify the identity of its clients in such manner and subject to such conditions as may be prescribed.
d. Identity the beneficial owner, in any, of such of its clients, as may be prescribed;
e. Maintain record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.

The Prevention of Money Laundering Rules (PML Rules) has been framed under the PMLA. Rule 3 of the PML Rules specifies the transactions, the records of which are to be maintained. Rule 7 of the PML Rules prescribes the procedure and manner of furnishing information, including an obligation to evolve an internal mechanism for detecting the prescribed transactions. Rule 8 of the PML Rules prescribes the time of furnishing such information and Rule 9 of the said Rules prescribes the procedure and manner of verification of records of identity of clients.

The Bank, its Designated Directors on the Board, Principal Officer and employees are responsible for omissions and commissions in relation to the reporting obligations under Chapter IV of the PMLA.

Rule 7 (1) of the PML, Rules requires that every RE should communicate to Director, FIU-IND, the name, designation and address of the Designated Director and the Principal Officer. Rule (2) (1) (ba) of the PML Rules defines "Designated Director" to mean a person designated by the reporting entity to ensure overall compliance with the obligations imposed under Chapter IV of the Act and the Rules and includes:-

i. the managing Director or a whole time Director duly authorized by the Board of Directors if the reporting entity is a company,
ii. the managing partner if the reporting entity is a partnership firm,
iii. the proprietor if the reporting entity is a proprietorship concern,
iv. the managing trustee if the reporting entity is a trust
v. a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and
vi. Such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above.

The role of the Designated Director is to ensure overall compliance with the obligations imposed under Chapter IV of the PMLA and to keep the Board informed of the AML/CFT issues. The role of the Principal Officer is to furnish all information to director, FIU-IND under Rule 7 and 8 of the PML Rules. Thus the role of the Designated Director is larger and includes all obligations under Chapter IV of the PMLA.

## KYC STANDARDS

The objective of the KYC Guidelines is to prevent Bank from being used intentionally or un-intentionally by criminal elements for Money Laundering Activities. KYC procedures and its compliance enable Banks to know and understand their customers and their financial dealings better which enables the Bank to manage Risk prudently. Our Bank in the year 2014 has once again taken initiative to comply with the KYC Norms by Data Entry and follow ups of customers for related documents in accordance with the laid down guidelines.

## AML

Concealing the existence or source of income from a crime disguising the income so that it appears legitimate. Whosoever directly or indirectly attempts assisting or knowingly is a party or is actually involved in any process of moving money, property, that constitutes the proceed of criminal activity shall be guilty of offence of Money Laundering.

Money Laundering mainly refers to washing of the proceeds of the profit generated from drugs, bribery, trafficking criminal and corruption activity, smuggling, gambling, prostitution, counterfeiting terrorist act and forgery.

## HOW MONEY LAUNDERING WORKS:

1. False Export Import Invoices- showing loans- Creating Bogus Companies, Property Market, Agricultural Products (as there is not income tax and mostly the transactions are on cash basis, Stock Markets. Some of the Popular places from where money is laundered through

2. Lawyers, Accountants, Correspondent Banking Companies Trading and Business activity, Insurance and Personal Investment Products, Investment Banking and the Securities Sector, Credit/Debit Cards, Forex Money Changers, Loan Bank arrangements, Payable through accounts, connected accounts, Deposit structuring or smurfing, Typologies techniques employed & Misuse of Non Profit Organisation, Other intermediaries.

3. Financing of terrorism, Money to fund terrorist activities movers through the Global financial system via wire transfers and in and out of personal and business accounts it can sit in the accounts of illegitimate charities and be laundered through buying and selling securities and other commodities or purchasing and cashing out insurance policies. Although terrorist financing is a form of money laundering, it doesn't work the way conventional money laundering works. The money frequently starts out clean i.e. as a charitable donation before moving to terrorist accounts. It is highly time sensitive requiring quick response.

4. Collection of membership Financial of terrorism i) State Sponsored (ii) Other Activities- legal or non legal, Legal Sources of terrorist financing, Donation of a portion of personal savings, Appeal to wealthy members of the community, Door to door solicitation within community, Cultural of social events, Sale of publications dues.

5. Drug trafficking, thefts and robbery and misuse of non profit organization and charities fraud, Fraud including credit card fraud, Smuggling, Kidnap and extortion, Financing of terrorism, Illegal sources.

## WHAT ARE THE RISKS TO THE BANK:

1. Money Laundering Risks: i) Reputational risk (ii) Legal risk (iii) Operational risk (failed internal processes, people and systems and technology) (iv) Concentration risk (either side of balance sheet). All risks are inter-related and together have the potential of causing serious threat to the survival of the Bank.

2. Banks vulnerable to Reputational Risk as they can easily become a vehicle for or a victim of customers illegal activities. Reputational Risk, a major threat

to Banks as confidence of depositors, creditors and general market place to be maintained. The potential that adverse publicity regarding a Bank's business practices, whether accurate or not, will cause a loss of confidence in the integrity of the institution, Reputation Risk.

3. Weakness in implementation of Banks' programs, ineffective control procedures and failure to practice due diligence. The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events, Operational Risk.

4. Bank can suffer fines, criminal liabilites and special penalties imposed by supervisors, Banks may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practice due diligence. Thepossibility that lawsuits, adverse judgements or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or conditions of Bank. Legal Risk.

## CUSTOMER ACCEPTANCE POLICY

For the purpose of KYC Policy, a Customer may be defined as:

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

**Client accounts opened by professional intermediaries:**

REs shall ensure while opening client accounts through professional intermediaries, that:

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

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

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

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

e) REs 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) The ultimate responsibility for knowing the customer lies with the RE.

**Guidelines**

Following are the explicit guidelines given to ensure the customer relationship in the Bank.

i) No account is opened in anonymous or fictitious / benami name(s);

ii) Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorization of customers into low, medium and high risk;

iii) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the guidelines issued by Reserve Bank from time to time;

iv) Not to open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and/ or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of the data/information furnished to the bank. Such decision to close an account may be taken at Central Office after giving due notice to the customer explaining the reasons for such a decision, as a built in measure to avoid harassment of those customers;

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

vi) Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc. Branches are advised to prepare a profile for each new customer based on risk categorization.

The customer profile may contain information relating to customer's identity, social / financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the branch. However, while preparing customer profile, branches should take care to seek only such information from the

customer which is relevant to the risk category and is not disturbing. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorized as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulators and statutory bodies etc.

Customers that are likely to pose a higher than average risk to the bank may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Branches are advised to apply enhanced 'due diligence' measures based on the risk assessment, for higher risk customers, especially those for whom the sources of funds are not clear.

Examples of customers requiring higher due diligence may include :

(a) non-resident customers,
(b) high net worth individuals,
(c) trusts, charities, NGOs and organizations receiving donations,
(d) companies having close family shareholding or beneficial ownership
(e) firms with 'sleeping partners',
(f) politically exposed persons (PEPs) of foreign origin,
(g) non-face to face customers and
(h) those with dubious reputation as per public information available etc.

It is important to bear in mind by the branches that its implementation should not become too restrictive and must not result in denial of banking services to general public, especially to those, who are financially or socially disadvantaged.

## CUSTOMER IDENTIFICATION PROCEDURES

**What is Identity?**

Customer identification means identifying the customer and verifying his/her identity by using reliable independent source documents data or information. The Branches need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer and the purpose of the intended nature of banking relationship. Due diligence is to be observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based approach is considered necessary to avoid disproportionate cost to Banks and a burdensome regime for the customers.

For customers who are natural persons, the branches should obtain sufficient identification data to verify the identity of the customer, his address/location and also his recent photograph.

For customers who are legal persons or entities, the branches should (i) verify the legal status of the legal person/entity through proper and relevant documents, (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person and (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

**Identification of Accounts**

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

**What is Identification?**

Identification is the act of establishing who a person is.

In the context of KYC (Know your Customer), identification means establishing who a person purports to be. This is done by recording the information provided by the customer covering the elements of his identity (i.e. name and all other names used, and the address at which they can be located). Following are some of the documents which the branches can accept for establishing identity of a person: Passport Driving License Identity Card of any Institution PAN Card Voter's Identity Card Aadhar Card Other documentary evidence in support of the person's residential address in addition to the above.

**What is Verification?**

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

KYC Guidelines go beyond merely establishing the identity of the person and satisfying about his credentials. The due diligence expected under KYC invokes going into the purpose and reasons for opening the account, anticipated turn-over in the account, source of wealth (net-worth) of the person opening the account and the source of funds flowing into the account. While opening new accounts, the branches in addition to routine procedures, make their efforts to get documents for identification and proof of residence having present and permanent addresses along with telephone numbers etc., from the account-openers. Particulars of other accounts with any other banks, Permanent Account Number (PAN) given by Income Tax Authorities, Registration Certificate in the case of partnership firms and Certificate of Incorporation, Memorandum &

Articles of Association from Companies and Resolution by Boards for accounts of Companies should be obtained. The branches should prepare a customer profile containing the expected activities of his business. They should collect additional details such as:-

• Employment details such as job specifications, name and address of the employer, length of service etc.; • Details about source of income and annual income;

• Details of assets owned such as house, vehicle etc; • Other personal details such as qualification, marital status etc. This profile would give an idea of the expected transactions in the account as assessed /envisaged at the time of opening of the account.

Any suspicious activity can be compared with this profile. Features to be verified and documents to be obtained from customers .

**Features Documents**

Accounts of individuals

Legal name and any other names used.

Correct permanent address (i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving licence. (v) Identity card (subject to the bank's satisfaction) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of branch. (i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority (iv) Letter from employer (subject to satisfaction of the branches) (any one document which provides customer information to the satisfaction of the branch will suffice)

**Accounts of Companies**

Name of the company /Principal place of business /Mailing address of the company

Telephone/Fax Number

(i) Certificate of incorporation and

Memorandum & Articles of Association

(ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account

(iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf

(iv) Copy of PAN allotment letter (v) Copy of the telephone bill.

**Accounts of partnership firms**

Legal name /Address /Names of all partners and their address /Telephone numbers of the firm and partners.

(i) Registration certificate if registered

(ii) Partnership deed

(iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf

(iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses and
(v) Telephone bill in the name of firm/partners.

**Accounts of trusts & foundations**
Names of trustees, settlers, beneficiaries and signatories.
Names and addresses of the founder, the managers/directors and the beneficiaries.
Telephone/fax numbers.
(i) Certificate of registration, if registered
(ii) Power of Attorney granted to transact business on its behalf
(iii) Any officially valid document to identify the trustees, settlers and their addresses.

(iv) Resolution of the managing body of the foundation/association
Small account For persons not able to provide normal KYC
Account can be opened with a form filled up & signed before the bank officer with self-attested photograph – bank officer to certify Accounts to have limitations on credit/debit/balance Only at CBS-enabled branches No foreign remittances allowed and is valid Only for 12 months – further extension on application for Officially Valid Document .
Provided, the customer intends to keep the balance below Rs.50,000/-and total of credit transactions in the account is not to exceed Rs.1 lakh during a financial year. Customer should be made aware of the limits and consequence of exceeding the same
No further transactions will be permitted until the full KYC procedure is completed. The bank must notify the customer when the balance reaches Rs. 40,000/-) or the total credit in a year reaches Rs. 80,000/- and that appropriate documents for conducting the KYC must be submitted failing which operations in the account will be stopped
Account Opening Process: During the account opening process , deduping of the customers using submitted OVD's ( Officially valid Documents eg; PAN Card, Aadhar Card, Passport, NREGA, Driving Licence, Election Card) along with Date of Birth and address which ever to avoid multiple relationship identification numbers.
Adherence to the laid down KYC policies
Scrutiny of documents by risk containment unit (RCU)
For authenticity of documents
Physical verification by adopting risk based approach.
To obtain sufficient information necessary to establish, to their satisfaction, the identity of customer and the purpose of the intended nature of banking relationship.
**On-going Due Diligence**

REs shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the 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:

a) 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.
b) Transactions which exceed the thresholds prescribed for specific categories of accounts.
c) High account turnover inconsistent with the size of the balance maintained.
d) Deposit of third party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

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

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

(a) A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.
(b) The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

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

**RISK PROFILING:**

The Reserve Bank of India Master Circular dated July 01, 2009 on Know Your Customer Norms / Anti Money Laundering Standards which consolidates all guidelines issued on the subject requires banks to categorize customers into low, medium and high risk categories and have different due diligence and monitoring standards based on risk assessment.

Following the steps described above should allow you to master the task of designing a risk-based approach to achieve compliance with PMLA 2002 It gives you the EXPLICIT GUIDELINES TO ENSURE THE CUSTOMER RELATIONSHIP IN THE BANK:

Though the bank has integrated them into a more automated approach.in AML software for compliance.

| | LOW- 1 | PT -1 | MEDIUM-2 | PT -2 | HIGH-3 | P T-3 |
|---|---|---|---|---|---|---|
| CATEGORY-1 Client Type | Student/Housewife/Pensioner | | Employee-Executive –Govt. | | | |
| | Employee/Non-Executive Govt. | | Lawyer & Accountant | | PEPs | |
| | Employee/Non-Executive Private | | Govt. Institutions | | NGOs | |
| | Public Ltd.Liability Co. | | Private Limited Liability Co. | | Offshore/Non Resident Co. | |
| | Business-Individual | | Business Proprietor/Partnership | | Foreign Citizen | |
| | Club/Society/Association | | | | | |
| | Educational Inst. | | | | | |
| | Self Employed-Professional | | | | | |
| | Self Emp.Business | | | | | |
| | Other Individuals | | | | | |
| CATEGORY-2 BUSI./ TRADE/ USAGE | Professional/Family Use Dealer in Petroleum | | Travel Agent | | Dealer/Trader in Gem & Jewellery | |
| | Professional Service | | Importer & Dist. Of Commercial Goods | | Finance/ Insurance Companies | |
| | Dealer in brand new vehicles | | Enterpot Trade | | Money Changers/ Remitters | |
| | Retail Traders/Business | | Exporter of Local Product | | Buying & Selling of Real Estate. | |
| | Service Provider | | Telephone/Communication Providers | | Share & Stock | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | brokers | |
| | Printer & Publisher | | Commission Agent | | Investing/Administering/Mg.Public Funds | |
| | Marketing & Advt | | Wholesale Trader | | Restaurant /Bar/Casino/Gambling House/Night Club | |
| | Small/Medium work shop/Repair Shop | | Shipping Airline & Freight Forward | | Importer/Dealer in 2nd Hand Motor vehicles. | |
| | Nursing Homes/Health Care Centres | | Construction-Building/Roads | | | |
| | Mfg. Industry/Transport Operations | | | | | |
| | Social Religious Activities | | | | | |
| CATEGORY -3 TURNOVER PER MONTH | Less than 1,000,000/- | | From 1,000,000 to 3,000,000 | | Above 3,000,000 | |

| | | Screening Frequency |
|---|---|---|
| Overall Rating 1- 3 Low | | Annually |
| 4 – 6 Medium | | Quarterly Screening |
| 7 – 9 High | | Fortnightly screening |

Regular screening is necessary to ensure that a client who is not known to be a PEP, or a money launderer, at the time when the account was opened, does not become such in the course of the relationship.

Parameters used for rating:
Product :
Customer type
Country of residence
Account status (Dormant, Inactive, Active)

Status of customer (HNI, Salaried, etc)

Occupation

Industry

Location

No. of alerts generated in account

STR filed for the account

Automated model supported by manual over-rides

Name Screening

Name screening processes

Account opening

Cross border transactions

Screening of legacy customers at frequent intervals

Negative list database

Database sourced from internationally acclaimed vendors

Augmented by internally developed lists

Suite of lists include UN, RBI list etc.

**Suspicious Transactions**:

1. Suspicious Transactions means a transaction whether or not made in cash which, to a person acting in good faith, gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime or appears to be made in circumstances of unusual or unjustified complexity or appears to have not economic rationale or bonafide purpose.
2. Corporate accounts where deposits or withdrawals are primarily in cash.
3. Corporate accounts where deposits, withdrawals and remittances, transfers from/made to sources apparently unconnected with the corporate business activity/dealings.
4. Unusual applications for D.D/T.T./P.O. against cash.
5. Accounts with large volume of credits through D.D./T.T./P.O.
6. A single substantial cash deposit composed of many high denomination notes.
7. Frequent exchanges of small denomination notes for large denomination notes or vice- versa.
8. Multiple accounts under the same name and sudden surge in activity level.
9. Sending or receiving frequent or large volumes of cross border remittances.
10. Remittances received by T.T./D.D./P.O. from various centers and in turn remitting the consolidated amount to a different account/centre on the same day leaving minimum balance in the account.
11. Employees leading lavish lifestyles that do not match their known income sources, sudden increase in cash deposits of an individual with no justification Large cash withdrawals from a dormant or inactive account or

account with unexpected large credit from abroad, providing misleading information/ information no easily verifiable while opening an account .

12. Reluctance to provide normal information when opening an account or providing minimal or fictitious information. Receipt or payment of large cash sums with no obvious purpose or relationship to Account holder/ his business. Substantial increase in turnover in a dormant account. Large cash deposits into same account.
13. Changing the firm of money, Control over money, Concealing true ownership and origin of money, Provide anonymity, Disguise the audit trail, Role of cash in money laundering.
14. All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month. All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency.
15. Suspicious Transaction Report within 7 days of arriving at a conclusion that any transaction is of suspicious nature. Cash Transaction Report by the 15th of the succeeding month (individual transactions below rupees fifty thousand may not be included DUE DATES.

**Guidelines on detecting suspicious transactions under Rule 7(3) of the Prevention of Money Laundering.**

The IBA Parameters and FIU Guidance note on KYC is circulated to all departmental Head , Branches separately .

**General**

The Prevention of Money Laundering Act, 2002 (PMLA) brought into force with effect from 1st July, 2005, is applicable to all the Reporting Entities (RE) as defined in the said Act. Section 12 of the PMLA places certain obligations on the reporting entities which are as follows:

(a) Maintain a record of all transactions, including information relating to transactions covered under clause (b), in such manner as to enable it to reconstruct individual transactions;

(b) Furnish to Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value as may be prescribed.

(c) Verify the identity of its clients in such manner and subject to such conditions as may be prescribed.

(d) Identity the beneficial owner, in any, of such of its clients, as may be prescribed;

(e) Maintain record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.

The RE, its Designated Directors on the Board and employees are responsible for omissions and commissions in relation to the reporting obligations under the PMLA.

The rule requires that every RE should communicate to Director, FIU-IND, the name, designation and address of the Designated Director and the Principal Officer. "Designated Director" to mean a person designated by the reporting entity to ensure overall compliance with the obligations imposed under Chapter IV of the Act and the Rules and includes:-

(i) the managing Director or a whole time Director duly authorized by the Board of Directors if the reporting entity is a company,

Principal Officer is defined an officer designated by a RE.

The role of the Designated Director is to ensure overall compliance with the obligations imposed under Chapter IV of the PMLA and to keep the Board informed of the AML/CFT issues. The role of the Principal Officer is to furnish all information to director, FIU-IND under.

The reporting entities are advised to generate any other alert, as they deem fit, to track suspicious transactions based on the definition of suspicious transactions as given and also based on maintenance of records of transactions.

1. **Detection and furnishing information in respect of suspicious transactions**

**Relevant Rules under the PML Rules**

The PML Rules empowers the Director, FIU-IND to issue guidelines in consultation with the regulator with regard to transactions pertains to suspicious transactions.

The terms "transaction" and "suspicious transaction" have been defined in the Prevention of Money Laundering Rules (PML Rules) as follows:

**Transaction** is defined under Rule 2(h) of the PML Rules and means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes-

(i) Opening of an account

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

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

(iv) Entering into any fiduciary relationship.

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

(vi) Any payment made in respect of playing games of chance for cash or kind including such activities associated with casino and.

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

**Suspicious transaction** is defined and means a transaction whether or not made in cash which, to a person acting in good faith-

gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or

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

(ii) appears to have no economic rationale or bonafide purpose; or

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

The PML Rules provides the timelines for reporting of transactions to FIU-IND. Tthe Principal Officer of a RE is required to furnish the information regarding a suspicious transaction not later than seven working days on being satisfied that the transaction is suspicious.

**Detecting suspicious transactions**

**Alert Generation**

Alert generation is a process by which the preliminary details of suspicious/unusual transactions are generated to enable the Principal Officer (PO) to analyse and review the details and arrive at a conclusion as to whether a transaction is suspicious.

An alert is the first step in identification of a suspicious transaction and is a red flag which is generated arising out of a transaction. Once the alert is generated, it has to be analysed to confirm whether the transaction is ultimately suspicious or not based on the above definition.

**Reporting Requirements to Financial Intelligence Unit – India**

REs shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records)Rules, 2005 in terms of Rule 7 thereof.

Explanation: In terms of Third Amendment Rules notified September 22, 2015regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the REs for detecting transactions referred to in

various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

The reporting formats and comprehensive reporting format guide, prescribed / released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by REs which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Principal Officers of those REs, whose all branches are not fully computerized, shall have suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in. .While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a misrepresented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. REs shall not put any restriction on operations in the accounts where an STR has been filed. REs shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level. Robust software, throwing alerts when the transactions are inconsistent

with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

**Source of Alert**

i. **System Dependent:** A Cooperative Bank must have system in place to generate alerts based on certain threshold on the transactions of the client to identify suspicious transactions.

ii. **System Independent:** All Co-operative Banks need to have a mechanism of raising alerts/triggers from employees, media reports, law enforcement agency queries etc. Efforts should be made to create awareness on reporting of unusual transactions.

### 2.3.3 Review and Management of Alerts

An element of subjectivity and application of mind of the Principal Officer (PO) is involved in the decision making process for reporting suspicious transactions. The PO is expected to gather as much information as possible from all relevant sources, to arrive at the decision on an alert. The PO and the staff assisting him in execution of AML/CFT guidelines should have timely access to customer identification data, other KYC information and records.

While the activities of analysing alert and preparing the documents for managing the alert can be delegated within the AML compliance team, the ultimate analysis and decision making rests with the PO. The records verified by and papers related to this decision need to be recorded and retained for audits.

Where the PO is of the opinion that a transaction is not reportable, decision on closure and reporting should be taken by the PO and it must be ensured that reason for not reporting the suspicious transactions are clearly recorded.

An independent review of the process of generation of alerts by an independent person, would confirm whether all the alerts which are required to be generated, are indeed generated as per the rules. The responsibility of deciding on the alerts and reporting/non-reporting of the Suspicious Transactions to FIU-IND cannot be delegated to any regional team members as there is a risk of the information being tipped-off.

The PO also needs to review the list of alerts and the approach from time to time to ensure that the reporting mechanism is complete and is in line with the expectations. It is equally important that the PO conducts surprise checks of the data being monitored by the AML compliance unit and check few random transactions to ensure that there is no gap and all unusual transactions have been indeed highlighted to the PO on a regular basis.

## ILLUSTRATIVE EXAMPLES OF 'GROUNDS OF SUSPICION'

The following are some of the illustrative examples of 'Grounds of suspicion' which may lead to a conclusion about the suspicious nature of the transaction (these are covered by the RBI in its various circulars or IBA guidelines)

i) If a branch has reason to believe that a customer is intentionally structuring any transaction into a series of transactions below the threshold of Rs. 50000/- (Rupees fifty thousand). The branch should verify identity and address of customer and also consider filing a Suspicious Transaction Report (STR).

ii) In the circumstances when a branch believes that it would no longer be satisfied that it knows the true identity of the account holder, the branch should also file an STR.

iii) Branches should pay special attention to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the branch. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. **High-risk** accounts have to be subjected to intensified monitoring.

iv) Branch should exercise ongoing due diligence with respect to the business relationship with every client & closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds.

v) If a branch has reason to believe that a customer is intentionally structuring wire transfer to below Rs.50000/- (Rupees fifty thousand) to several beneficiaries in order to avoid reporting or monitoring, the branch must insist on complete Customer Identification before effecting the transfer. In case of

non-cooperation from the customer, efforts should be made to establish his identity and STR should be made.

vi) Wire transfers lacking complete originator information shall be identified and this must be considered as a factor in assessing whether a wire transfer or related transactions are suspicious. If they are found to be of suspicious nature then STR to be created.

vii) "Money Mules" can be used to launder the proceeds of fraud schemes (e.g. phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "Money Mules." The operations of mule accounts can be minimized if branches follow the guidelines contained in the RBI Circulars on KYC. Branches are, therefore, advised to strictly adhere to the guidelines on KYC issued and to those relating to periodical updation of Customer Identification data after the account is opened. Branches are also required to monitor transactions in order to protect themselves and their customers from misuse by such fraudsters.

viii) Branches are required to apply enhanced due diligence measures on 'high' and 'medium' risk customers. Accordingly, branches are also required to subject these 'high and medium risk accounts' to intensified transaction monitoring. Higher risk associated with such accounts should be taken into account by the branches to identify suspicious transactions for filing STRs.

ix) It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. The branches should report all such attempted transactions in STRs, even if not completed by customers. These should be reported irrespective of the amount of the transaction. Branches should raise STRs if they have reasonable ground to believe that the transaction involves proceeds of crime irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences

x) The transactions that give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism should also be reported.

xi) When a business relationship is already in existence & it is not possible to perform Customer Due Diligence on the customer in respect of the business relationship STR to be created.

xii) Accounts of persons under investigation by any regulatory authority should be reported as suspicious.

xiii) It is imperative that the bank has a system in place, which will ensure that the account of the person of any dubious back ground is not opened or any suspicious transaction if routed through the branch will be identified. The CIP module of the AML package throws the alerts, if the name of the accountholder is similar to the name of the persons enumerated in the various lists uploaded in the system (UN sanctioned Terrorist list, Mumbai Police List, RBI cautioned list of exporters). If the branches are unable to establish if the true identity of the account holder is different from the name appearing in the list, then the same need to be reported as STR.

**Subjective test for identifying suspicious transactions:**

The review of pattern of transactions in the account and other related information provides an insight into intended purpose of the transaction. Examples where such review can assist in meeting the subjective test that 'gives rise to reasonable ground of suspicion' is as follows:

i) Transaction pattern are not consistent with normal business, personal, remittance or tourist spending activity. For eg: High value transactions in the account of a maid servant, tailor etc.;

ii) The amounts or frequency or the stated reason of the transaction does not make proper business sense or not commensurate with the profile of the customer, say student, etc.;

iii) Large number of transfers received at once or over a certain period of time which is much greater than what would be expected for such a receiver;

iv) Unrelated sender or receiver;

v) Customer who travels unexplained distances to conduct transactions;

vi) Migrant remittances made outside the usual remittance corridors;

vii) Personal funds sent at a time not associated with salary payments;

viii) Several accounts with same authorized signatories/introducer;

ix) Cash deposited and transferred to own account with other bank or veceversa;

x) Property transactions though cheque/RTGS in a newly opened account;

xi) Walk in customer especially saying that he does not have any bank account till date;

It should be ensured that the business transactions are not routed through other than the business accounts. eg: Business transactions routed through savings account should be treated as suspicious

1. Continuous improvements

BOMBAY MERCANTILE CO-OPEARTIVE BANK LTD will continuously improve the risk management program on anti-money laundering and countering the financing of terrorism measures through periodical review and internal audit. Also, the BOMBAY MERCANTILE CO-OPERATIVE LTD will develop forward-looking actions for strengthening its anti-money laundering and countering the financing of terrorism measures to prevent the future misuse of the Group's business.

## KNOW YOUR CUSTOMER (KYC) GUIDELINES

"KYC" is the platform on which the banking system operates to avoid shortcomings in operational, legal and reputation risks to the institution and the consequential losses by scrupulously following various procedures laid down for opening and conduct of accounts.

The "KYC" guidelines are as follows and they help the institution from using the banking channel for illegal financial activities.

- To detect suspicious activity in a timely manner,
- To promote compliance with all banking laws,
- To promote safe and sound banking practices,
- To eliminate the risk that the bank will be used for illicit activities,
- To reduce the risk of government seizure and forfeiture of a client's loan collateral when the customer is involved in criminal activity.
- To protect the Bank's reputation.-
- To minimize frauds.
- To obtain protection under Section 131 of Negotiable Instruments Act 1881,
- To check misappropriations,
- To weed out undesirable customers,
- To avoid opening of accounts with fictitious names and addresses
- To monitor transactions of suspicious nature.

In line with the Know Your Customer (KYC) guidelines accepted as anti-money laundering measure, its objective is to ensure appropriate customer identification and to monitor transactions of a suspicious nature. It should be ensured that the procedure adopted does not lead to denial of access to the general public for banking services. Ongoing monitoring is an essential element of effective KYC procedures. The branches can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extend of monitoring will depend on the risk sensitivity of the account. The branches should pay special attention to all complex, unusually large transactions and unusual patterns which have no apparent economic or visible lawful purpose. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the branch. The branches should take note that high account turn over inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. The branches should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors.

Necessary precautions should be taken when cheque/draft/ dividend/refund order/interest warrants bearing a date of issue prior to the opening of the Account are presented by the account holder for credit of new account. In such cases, the bona-fides of ownership of such instruments should be got satisfied.

While accepting such instruments for collection, the relevant information such as purpose towards which it was received by the account holder, whether he has any previous bank account, and if so, the necessity of opening this account etc. should be gathered.

Caution should be exercised whenever cheques/ drafts for large value, are presented for collection in a newly opened account (s) immediately / within short period of the opening date thereof. This shall be applied in case of inward remittance by way of TTs and other transactions.

Any instruments for large amount received for collection in the account should put the branch on extra care. Inquiries should be made with the account holders as to the nature of transaction and sources of receipt of such payments.

KYC Guidelines go beyond merely establishing the identity of the person and satisfying about his credentials. The due diligence expected under KYC invokes going into the purpose and reasons for opening the account, anticipated turn-over in the account, source of wealth (net-worth) of the person opening the account and the source of funds flowing into the account. While opening new accounts, the branches in addition to routine procedures, make their efforts to get documents for identification and proof of residence having present and permanent addresses along with telephone numbers etc., from the account-openers. Particulars of other accounts with any other banks, Permanent Account Number (PAN) given by Income Tax Authorities, Registration Certificate in the case of partnership firms and Certificate of Incorporation, Memorandum & Articles of Association from Companies and Resolution by Boards for accounts of Companies should be obtained. The branches should prepare a customer profile containing the expected activities of his business. They should collect additional details such as:-

• Employment details such as job specifications, name and address of the employer, length of service etc.; • Details about source of income and annual income;

• Details of assets owned such as house, vehicle etc; • Other personal details such as qualification, marital status etc. This profile would give an idea of the expected transactions in the account as assessed /envisaged at the time of opening of the account.

Any suspicious activity can be compared with this profile. Features to be verified and documents to be obtained from customers

**CEILING AND MONITORING OF CASH TRANSACTIONS:-**

Travellers cheques, Demand drafts, Mail transfer and Telegraphic transfers for Rs.50,000/- (approx USD 1100/-) and above are issued only by debit to customer's

accounts or against cheques and not against cash. Further, applicants for the above transactions for amount exceeding Rs.50,000/- While issuing demand drafts/payorders for amount Rs.20,000/- and more, if the applicant is not an account holder, are required to affix a photo copy of PAN Card should be filed with the application.

As per the "KYC", the identity of the customer is to be established and for issue of Demand Drafts etc. for Rs. 50,000/- and above is by debit to account of the purchaser /remitter.
The Bank keeps a close watch on integral cash Transaction above Rs 10.00 Lacs and above in deposits cash credit and overdraft account . and put in place a system of reporting all deposit & withdrawal of Rs 10.00 Lacs as well as transaction of suspicious nature with full details and maintain and review these records and verify compliance of guidelines in this regard.

## Risk Management

The bank has put in place an effective KYC programme in place by establishing appropriate procedures and ensuring their effective implementation covering proper management oversight, systems and controls, segregation of duties, training and other related matters.
Responsibility has also been explicitly allocated within the bank for ensuring that the bank's policies and procedures are implemented effectively. The nature and extent of due diligence will depend on the risk perceived by the branch/bank. However, while preparing customer profile branches should take care to seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.
Bank's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. It would be ensured that the audit machinery is staffed adequately with individuals who are well versed in such policies and procedures.

## Risk Based Approach

Identification of the money laundering risks of customers and transactions allows us to determine and implement proportionate measures and controls to mitigate these risks. The used risk criteria *inter alia* are the following:
**Transaction Based Risk**, Risk Rating Offshore Wire Transfer to High Risk Jurisdiction / Cash deposit under threshold/structuring transactions Large Cash Deposit Forex Early Loan Repayment .- **Country risk**, In conjunction with other risk factors, provides useful information as to potential money laundering risks. Factors that may result in a determination that a country poses a higher risk include:
- Countries subject to sanctions, embargoes or similar measures;
- Countries identified by the Financial Action Task Force ("FATF") as non cooperative in the fight against money laundering or identified by credible sources as lacking appropriate money laundering laws and regulations;

• Countries identified by credible sources as providing funding or support for terrorist activities;
• Countries identified by credible sources as having significant levels of corruption, or non-transparent tax environment.
*Customer risk* - there is no universal consensus as to which customers pose a higher risk, but the below listed characteristics of customers have been identified with potentially higher money laundering risks:
• Armament manufactures,
• Cash intensive business;
• Unregulated charities and other unregulated "non profit" organizations;
• Dealers in high value of precious goods;
• "Politically Exposed Persons" (frequently abbreviated as "PEPs"), referring to individuals holding or having held positions of public trust, such as government officials, senior executives of government corporations, politicians, important political party officials, etc., as well as their families and close associates;
*Services risk.* Determining the money laundering risks of services should include a consideration of such factors as:
• services identified by regulators, governmental authorities or other credible sources as being potentially high risk for money laundering;
• services involving banknote and precious metals trading and delivery

**Customer Due Diligence and Know Your Customer**

• Prior to transact any type of business BANK must determine and document the true identity of customers and obtain background information on customers as well as purpose and intended nature of the business;
• BANK must obtain and document any additional customer information, commensurate with the assessment of the money laundering risk using Risk Based Approach;
• BANK must establish whether the Customer is acting on behalf of another natural person or legal entity as trustee, nominee or professional intermediary. In such cases a necessary precondition for Customer acceptance is receipt of satisfactory evidence of the identity of any intermediaries and of the persons upon whose behalf they are acting, as well as the nature of the trust arrangements in place.

**Additional Due Diligence measures for financial institutions**

• BANK must undertake following additional due diligence measures while establishing and maintaining correspondent relationships:
Obtaining sufficient information about a respondent institution - Determining from publicly available sources of information the reputation of a respondent institution, including whether it has been subject to a money laundering or terrorist financing investigation or other regulatory action;
- Assessing the respondent institution's anti-money laundering and terrorist financing controls on a periodic basis;

**Enhanced and Simplified Due Diligence Procedure**

**Enhanced Due Diligence**

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

**Accounts of Politically Exposed Persons (PEPs)**

A. REs 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 REs' 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.

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

**Simplified Due Diligence**

**Simplified norms for Self Help Groups (SHGs)**

(a) CDD of all the members of SHG as per the CDD procedure mentioned in Section 15 of the MD shall not be required while opening the savings bank account of the SHG

(b) CDD as per the CDD procedure mentioned in Section 15 of the MD of all the office bearers shall suffice.

(c) No separate CDD as per the CDD procedure mentioned in Section 15 of the MD of the members or office bearers shall be necessary at the time of credit linking of SHGs.

**Procedure to be followed by banks while opening accounts of foreign students**

(a) Banks shall, at their 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.

**(i) <u>Periodic Updation :</u>**

Para 38 of the Master Direction requires that the periodic updation shall be carried out atleast 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 subject to the following procedure :

(a) The bank shall carry out

(i) PAN verification from the verification facility available with

the issuing authority;

(ii) Authentication of Aadhaar Number already available with the Bank with the explicit consent of the customer in applicable cases;

(iii) In case identification information available with Aadhaar does not contain current address an OVD containing current address may be obtained

(iv) Certified copy of OVD containing identity and address shall be obtained at the time of periodic updation from individuals not eligible to obtain Aadhaar, except from individuals who are categorized as low risk. In case of low risk customers when there is no change in status with respect to their identities and addresses is self-certification to that effect shall be obtained;

(v) In case of Legal entities, the bank shall review the documents sought at the time of opening of accounts and obtain fresh certified copies.

(b) The bank may not insist on the physical presence of the customers for the purpose of furnishing OVD or furnishing consent for Aadhar authentication unless there are sufficient reasons that physical presence of the account holders is required to establish their bonafides. Normally OVD / consent forwarded by the customer through mail / post etc. shall be acceptable.

(c) The bank shall ensure to provide acknowledgement with date of having performed KYC updation.

(d) The time limit prescribed above would apply from the date of opening of the account/last verification of KYC.

**(ii) <u>Periodic review of Risk Categorization of Accounts :</u>**

As per para 37 (a) of the Master Direction issued by RBI, UCBs are required to have a system of periodic review of Risk Categorization of

accounts with such periodicity being atleast once in six months and the need for applying enhanced due diligence measures shall be put in place. The extent of monitoring shall be aligned with the risk category of the customers i.e. high risk accounts have to be subjected to more intensified monitoring. The transactions in accounts of marketing firms, especially accounts of multi-level marketing companies shall be closely monitored. Cases where a large number of cheque books are sought by the company and/or multiple small deposits generally in cash across the country in one bank account and/or where a large number of cheques are issued bearing similar amounts / dates shall be immediately reported to Reserve Bank of India and other appropriate authorities such as FIU-IND.

**(iii)Prescribing preservation period of KYC documents :**

Para 46 of the Master Directions issued by RBI lays down following steps to be taken regarding maintenance, preservation and reporting of customer account information with reference to provisions of PML Act & rules.

The bank shall

(a) Maintain all necessary records of transactions between the bank and the customer, both domestic and international for atleast five years from the date of transaction.

(b) Preserve the record pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for atleast five years after business relationship is ended.

(c) Make available the identification records and transaction data to the competent authorities upon request.

(d) Introduce a system of maintaining proper record of transaction prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules 2005 (PML Rules 2005).

(e) Maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transactions including the nature of transaction, the amount of transaction and the currency in which it was denominated, the date on which the transaction was conducted and the parties to the transactions.

(f) Evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authority.

(g) Maintain records of the identity and addresses of their customers and records in respect of transactions referred to in Rule 3 in hard or soft format.

**Internal Control System**

Duties and responsibilities should be explicitly allocated for ensuring that policies and procedures are managed effectively and that there is full commitment and compliance to an effective KYC programme in respect of both existing and prospective deposit accounts. Zonal/Group Offices will periodically monitor strict adherence to the laid down policies and procedures by the officials at the branch level.

**Terrorism Finance**

Lists of terrorist entities, as notified by the Govt. of India, are communicated to all the Zonal/Group Offices, so that branches may exercise caution if any transaction is detected with such entities. The branches should ensure that such lists are consulted with their controlling authorities in order to determine whether a person/organization involved in a prospective or existing business relationship appears on such a list. Branches should report accounts suspected to belong to terrorist entities or transactions of suspicious nature, to the Principal Officer at Central Office.

**Internal Audit/Inspection**

Bank's internal audit and compliance functions have an important role in Evaluating and ensuring adherence to the KYC policies and procedures.

To ensure better execution of KYC / AML procedures and putting in place a sound monitoring mechanism in relation to the same, HO:Inspection Department is given the responsibility of handling the execution/monitoring aspects of KYC norms and AML measures including risk profiling of customers. The Department should ensure that their inspection machinery is staffed adequately with individuals who are well versed in KYC/AML policy and procedures. Concurrent/Internal Auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard should be put up before the Audit Committee of the Board on quarterly intervals

- The Group AML Center must be informed about all suspicious transaction/activity on a monthly basis;

**Record keeping and Record Management.**

• Records must be kept of all documents obtained for the purpose of identification and all transaction data as well as other information related to money laundering The following steps shall be taken regarding maintenance, preservation and reporting of customer account information, with reference to provisions of PML Act and Rules. REs shall,

(a) maintain all necessary records of transactions between the RE and the customer, both domestic and international, for at least five years from the date of transaction;

(b) preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;

(c) make available the identification records and transaction data to the competent authorities upon request;

(d) introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);

(e) maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:

(i) the nature of the transactions;

(ii) the amount of the transaction and the currency in which it was denominated;

(iii) the date on which the transaction was conducted; and
(iv)the parties to the transaction.
(f) evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quicklywhenever required or when requested by the competent authorities;
(g) maintain records of the identity and address of their customer, and records in respect of transactions referred to in Rule 3 in hard or soft format.

**Training**

• Training on anti-money laundering must be provided to those new employees who work directly with customers and to those employees who work in other areas that may be exposed to money laundering and terrorist financing threats;

• Follow-up trainings must take place not less than once a year

The bank shall ensure that the training sessions on KYC guidelines and AML & CFT procedures are included in the Training Calendar on an ongoing basis. The Bank shall arrange to update and modulate these training sessions to the requirements of front-line staff, compliance staff and counter-staff dealing with new customers. It shall be the bank's focussed endeavour to make all those concerned fully understand the rationale behind the KYC/AML & CFT procedures and implement them consistently.

• The Bank's operational staff shall continue to have the conviction to educate and impress the customers that the KYC guidelines are meant for good understanding and for better deliverance of customer service as also for weeding - out the fraudsters in the initial stage itself.

• Transaction monitoring with a view to detect suspicious cases is the most crucial problem that any comprehensive Anti-Money Laundering and Combating Financing of Terrorism measures must address. This fact is effectively taken care of by the structured methodology for implementing KYC/AML & CFT procedures which eventually tend to emit warning signals wherever required and the sustained functional commitment to these procedures in their day-to-day work will

enable desk officials to pick-up the adverse signals for reporting to Branch Manager through STR Reports. Customer Education

- In order to educate customers on KYC requirements and the need for seeking certain personal information from the customers/applicants for opening accounts and also to ensure transparency, the bank shall publish this Policy in the Bank's web-site and place a copy of the same in all branches/offices for the reference by user Public.

- It is the duty and responsibility of Operational Staff to educate the customers and tactfully/convincingly explain the need for customer profile and its relevance in the present adverse conditions of Money Laundering, Terrorist Financing etc. The customers shall be impressed upon the fact that the profile format enables the branch to render better Customer Service.

- An initial resistance by the customers to fill up the exhaustive customer profile format is an expected initial response and it is foreseen as a temporary phenomenon only. The expected resistance could be overcome if the background could be explained to the customers so that the required information can be gathered.

- The Bank shall endeavour to guard against denial of banking services to general public especially to those who are financially/socially under-privileged due to the implementation of Customer Acceptance Procedures on too restrictive basis.

The Bank Provides employee Training on Prevention of Money Laundering and Terrorisim Financing and also communicates new AML laws or changes in AML policies to relevant employees.

**Secrecy Obligations and Sharing of Information:**

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

(b) While considering the requests for data/information from Government and other agencies, banks shall satisfy themselves that the information being sought

is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.

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

i. Where disclosure is under compulsion of law

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

iii. the interest of bank requires disclosure and

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

(d) NBFCs shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.

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

REs 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 authorized 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.

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

(i) Scheduled Commercial Banks (SCBs) 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. SCBs are, however,33 allowed time upto February 1, 2017 for uploading date in respect of accounts opened during January 2017.

(ii) REs other than SCBs shall upload the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017 with CERSAI in terms

of the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

(iv) Operational Guidelines (version 1.1) for uploading the KYC data have been released by CERSAI.

(v) Further, 'Test Environment' has also been made available by CERSAI for the use of REs.

**Aadhaar eKYC (BIO)**

Aadhaar ekyc is a paperless Know Your Customer (KYC) process, wherein the Identity and Address of the subscriber are verified electronically through Aadhaar Authentication It can be used

as an alternate to current KYC process which is done on the basis of physical photocopies of the original documents (ID proof and Address proof).

According to Identity Verification Guidelines of CCA, the normal KYC process requires paper documents to be submitted, which should contain the attestation by Gazetted Officer / Bank Manager / Post Master. Subsequently CA should also carry out Mobile verification, Email Verification, Prerequisites for Aadhaar eKYC (Biometric Based Authentication)

To perform Aadhaar eKYC, subscriber should be physically available, and also facilitated with a biometric device. With this, a subscriber can perform Aadhaar eKYC either at RA location or any other place having the device.

To know more on Aadhaar eKYC, please contact the EDP department as the Aadhaar e-KYC process is not operational .

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

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

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

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

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

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

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

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

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

a) updated Guidance Note on FATCA and CRS

b) a press release on 'Closure of Financial Accounts' under Rule 114H

Difference between FATCA & CRS at a glance.Before talking about FATCA-CRS compliance, let us understand the difference between the two.

The US Tax Department launched FATCA in 2010 to promote tax compliance and discourage tax evasion. It stands for Foreign Account Tax Compliance Act. On the other hand, CRS is roughly a more international version of FATCA. While

the former is only for US persons, the latter is applicable for citizens of every registered country.

Therefore, both FATCA & CRS prevent offshore investors from avoiding tax and hoarding unaccounted cash overseas. This required cooperation from the tax authorities from all the G20 and OECD countries. Hence, they introduced a Common Reporting Standard or CRS.

| FATCA | CRS |
|---|---|
| Needs the help of a financial institution to find US persons | CRS has 90 countries (except the US) committed to it – has a wider scope |
| It is not compulsory to report on financial accounts always | Reporting your financial accounts is mandatory under CRS |
| Individual account should have more than $50,000 balance | No that's too small or insignificant to be of importance limit under CRS |
| Number of US people reported under FATCA are only a few thousands | Several millions of accounts are reported under CRS |

**Foreign Account Tax Compliance Act**

FATCA came into being to combat tax evasion and to ensure strict adherence to tax rules. Its main objective is to identify and prevent offshore tax avoidance by US citizens or residents. In short, an attempt to track US persons earning from overseas investments and stash assets in other countries!

FATCA enables financial institutions to withhold tax if the US persons refuse to meet the documentation requirements. For this, all financial institutions registered under this Act should immediately notify the US tax department when they come across US persons attempting to evade tax. Hence, all FATCA registered banks report such account holders (with the available information) immediately. This Act has a direct and profound impact on US multinationals and Foreign Financial Institutions.

**US-India agreement to implement FATCA**

FATCA ensures tax compliance and transformation at a global level. It presents foreign financial institutions a chance to improve and streamline their tax reporting process. It also gives them visibility in the foreign country and gains the trust of investors.

To accommodate FATCA, the government had inserted Rules 114F to 114H and Form 61B in the Income Tax Act in 2014. Then the Indian Government signed the Inter-Governmental Agreement (IGA) with the USA in 2015 for

implementation of FATCA. According to this agreement, Indian tax officials must obtain certain account information from US taxpayers. The goal was to ensure tax compliance by US citizens and increasing transparency for their Internal Revenue Service (IRS). This gave a legal basis for the Reporting Financial Institutions to maintain and report personal and income details.

**FATCA declaration for NRIs**

From January 2016, they made it mandatory for all Indian and NRI investors (existing and new) to file a FATCA self-declaration. While the details might be slightly different with each financial institution, the common info they mandate are:

a. Name
b. Permanent Account Number (PAN)
c. Address
d. Place (city/state) of birth
e. Country of birth
f. Nationality
g. Gross Annual Income
h. Occupation
i. Whether the resident of another country? If yes, then the country of residence, Tax ID number, and type

The declaration specifically asks to include the USA as a country of residence if you are a US citizen or a green card holder. This holds true even if you have moved to India and are now an Indian resident. Further, this declaration specifies that the Central Board of Direct Taxes (CBDT) has already covered this issuance in the rules 114F-114H. As a result, the tax authorities will have access to all relevant information. Therefore, please intimate the respective financial institution within 30 days in case of any change in the above information.

**Common Reporting Standard or CRS**

The Organization for Economic Cooperation and Development (OECD) developed a Common Reporting Standard (CRS) for Automatic Exchange of Information (AEoI). CRS mandates financial institutions across countries to provide respective tax authorities information about their citizens and their wealth overseas. This can help governments obtain information of financial assets held by its citizens internationally – for tax reasons. So far, more than 90 countries have agreed to follow this global standard.

India too signed a multilateral agreement to transfer personal and account information of another country's citizen to their respective tax authority. The Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters under the CRS rules refers to this.

**CRS Declaration**

Most of the details mandated under CRS self-declaration are similar to that of FATCA. However, CRS covers taxpayers from over 90 countries, as opposed to FATCA, which is for US taxpayers only. You can download the CRS self-declaration form from any offshore mutual fund website. Alternatively, you may visit the fund house service centers or the Asset Management Company (AMC) office itself.

Submit this self-declaration either online or offline at any of the fund company branches. For instance, Registrar and Transfer Agencies like CAMS offer this service. To complete the registration, you must enter the OTP, generated using your PAN number. Basically, CRS declaration is nothing but an extension of the Know Your Customer (KYC) documents.

Documents for FATCA & CRS declarations

All foreign financial institutions in India mandates US persons to submit the following documents.

a. PAN Card

b. Passport

c. Government-issued IDs like Voters ID or Aadhaar

The Government of India will identify the investor as a resident or an NRI on this declaration. Central Board of Direct Taxes (CBDT) will release notifications for all NRI investors on the necessary information.

Tax-evasion is not a problem unique to one country. Hence, the solutions should also be at a global level. The focus is more on the global transparency and consistency of compliance among the registered nations. In essence, FATCA and CRS have indeed gone a long way in reducing tax evasions and non-compliance globally in the recent years. Therefore, US persons including NRI investors should be aware of these regulations, especially if they are planning to invest in offshore funds.

**Introduction of New Technologies –Credit Cards/Debit Cards/Smart Cards/Gift Cards/Mobile Wallet/ Net Banking/ Mobile Banking/RTGS/ NEFT/ECS/IMPS etc.**

Adequate attention shall be paid by REs 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.

**64. Correspondent Banks**

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.

**65. Wire transfer**

REs 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.

**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.

**Hiring of Employees and Employee training**

(a) Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place.

(b) On-going employee training programme shall be put in place so that the members of staff are adequately trained in AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the RE, regulation and related issues shall be ensured.

**Adherence to Know Your Customer (KYC) guidelines by NBFCs/RNBCs and persons authorised by BFCs/RNBCs including brokers/agents etc.**

(a) Persons authorised by NBFCs/ RNBCs for collecting the deposits and their brokers/agents or the like, shall be fully compliant with the KYC guidelines applicable to NBFCs/RNBCs.

(b) All information shall be made available to the Reserve Bank of India to verify the compliance with the KYC guidelines and accept full consequences of any violation by the persons authorised by NBFCs/RNBCs including brokers/agents etc. who are operating on their behalf.

(c) The books of accounts of persons authorised by NBFCs/RNBCs including brokers/agents or the like, so far as they relate to brokerage functions of the company, shall be made available for audit and inspection whenever required.

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

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.

(A) Co-operative Banks shall 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.

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

Any remittance of funds by way of demand draft, mail / telegraphictransfer / 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.

**Quoting of PAN**

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

**68. Selling Third party products**

REs 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.

(e) Instruction at 'd' above shall also apply to sale of REs' 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.

**Collection of Account Payee Cheques**

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

(a) A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationships with individual customers as also the existing customers by banks and NBFCs.

(b)The banks/NBFCs shall, at their option, not issue UCIC to all walkin/ occasional customers such as buyers of pre-paid instruments/purchasers of third party products provided it is ensured that there is adequate mechanism to identify such walk-in customers who have frequent transactions with them and ensure that they are allotted UCIC.

**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.

**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

(a) launder the proceeds of fraud schemes (*e.g.*, phishing and identity theft) by criminals

(b) who gain illegal access to deposit accounts by recruiting third parties which act as

(c) "money mules." If it is established that an account opened and operated is that of a

(d) Money Mule, it shall be deemed that the bank has not complied with these directions

**Requirements / obligations under International Agreements**

**Communications from International Agencies –**

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.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.

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.

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

The procedure laid down in the UAPA Order dated August 27, 2009 (Annex I of this Master Direction shall be strictly followed and meticulous compliance with the Order issued by the Government shall be ensured.

**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 Res from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.*

(c) The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.

**Goals and objectives**

Adherence to this policy is absolutely fundamental for ensuring that all BRANCHES, regardless of geographic location, fully comply with applicable anti-money laundering legislation The HEAD OFFICE is committed to examining its anti-money laundering strategies, goals and objectives on an ongoing basis and maintaining an effective AML Policy for the bank's business.

**Parameter available in Software for Generation of Alerts:-**

a) File (UN Negative List upload option)
b) Master (Account type Management and whitelist reason Management)
c) CTR( Cash Transaction Monitoring and Reporting and generation of Report)

a) Maintaining a low or overdrawn balance with high activity
b) Multiple deposit of Mcs/DDs etc. followed by immediate withdrawal
c) same funds being moved repeatedly among several accounts
d) Sudden surge in activity level
e) Mutiple accounts under the same name
f) Large cash transactions
g) An account of a customer who does not reside/have office near to the branch even though there are bank branches near his office/residence
h) Depositing cash by means of numerous credit slip such that the amount of each deposit is not substantial but the total of which is substantial
i) Unexplained activity in dormant accounts

j) substantial cash withdrawals in accounts of charitable organization
k) Monitoring accounts of PEP(Politically exposed person)
l) Monitoring RTGS transactions
m) Monitoring accounts of jewellers
n) New account large transactions
o) Non Home Branch transactions
p) Monitoring accounts of staff
q) High Net worth
r) Customers with common phone numbers, mobile numbers
s) High value Transactions with PAN ID
t) Customers joint holder in multiple accounts
u) Structuring of deposit through multiple branches
v) Monitoring NEFT transactions
w) RTGS outward through same party
x) Monitoring of NEFT transactions
y) High value cheque Transactions(credit)
z) High Value cheque Transactions(debit)
1) High value Non cash Deposits in a Month
2) High value Non Cash withdrawals in a Month
3) Sudden High Value transactions for the client
4) Sudden increase in a value of transactions in a month of a client
5) High activity in new Account
6) High value cash transactions inconsistent with profile
7) High cash activity inconsistent with profile
8) Splitting of cash deposit below INR 10,00,000 in multiple accounts in a month
9) Splitting of cash deposit below INR 50,000
10) Frequent low cash deposits
11) Frequent low cash withdrawals
12) One to many fund
13) Repeated small cash deposits followed by Atm withdrawals in different locations
14) Repeated small value transfers from unreleated parties followed by immediate withdrawals
15) Large repetitive card usage at the same merchant
16) Repayment of loan in cash
17) Premature closure of large FDR through PO/DD
18) High number of cheque leaves
19) Frequent locker operations
20) High value cash transactions related to real estate
21) Inward remittances inconsistent with client profile
    - High value cash deposits in a day //////
    - High value cash withdrawals in a day
    - High value non-cash deposits in a day
    - High value non-cash withdrawals in a day

- High value cash deposits in a month
- High value cash withdrawals in a month
- High value non-cash deposits in a month
- High value non-cash withdrawals in a month
- Sudden high value transaction for the client
- Sudden increase in value of transactions in a month for the client
- Sudden increase in number of transactions in a month for the client
- High value transactions in a new account
- High activity in a new account
- High value transactions in a dormant account
- Sudden activity in a dormant account
- High value cash transactions inconsistent with profile
- High cash activity inconsistent with profile
- Splitting of cash deposits just below INR 10,00,000 in multiple accounts in a month
- Splitting of cash deposits just below INR 50,000
- Routing of funds through multiple accounts
- Frequent low cash deposits
- Frequent low cash withdrawals
- Many to one fund transfer
- One to many fund transfer
- Customer providing different details to avoid linkage

- Multiple customers working together
- Repeated small cash deposits followed by immediate ATM withdrawals in different location
- Repeated small value transfers from unrelated parties followed by immediate ATM withdrawals
- Repeated small value inward remittance from unrelated parties followed by immediate ATM withdrawals
- Repeated small value inward remittance from unrelated parties used for specified activities
- Majority of repayments in cash
- Repayment of loan in cash
- Premature closure of large FDR through PO/DD
- High number of cheque leaves
- Frequent locker operations
- High value transactions by high risk customers
- High value cash transactions in NPO
- High value cash transactions related to real estate

- High value cash transactions by dealer in precious metal or stone
- High value inward remittance
- Inward remittance in a new account
- Inward remittance inconsistent with client profile
- High value transactions with a country with high ML risk
- High value transactions with tax havens
- Transaction involving a country with high TF risk

Case examples, penalties and other risks associated.