THE SIRSI URBAN SAHAKARI BANK LIMITED, SIRSI – U. K.

POLICY GUIDELINES ON KYC/ AML/ CFT

1.0 OBJECTIVE

1.1 The objective of KYC/AML/CFT guidelines is to prevent Bank from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable Bank to know/ understand the customers and their financial dealings better and manage the risks prudently. The Board approved policy on KYC/AML/CFT is subject to annual review.

2.0 DEFINITIONS

2.1 Customer

For the purpose of KYC Norms, a 'Customer' is defined as a person who is engaged in a financial transaction or activity with the Bank and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting. Thus for the purpose of this policy customer may be defined as

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

The following guidelines are to be followed:

a. Branches should keep in mind that the information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes.
b. Branches shall ensure that any remittance of funds by way of demand draft, mail/ telegraphic transfer or any other mode for value of Rupees 50000/= and above is effected by debit to the customer's account or against cheques and not against cash payment.
c. Branches shall ensure that the provisions of Foreign Contribution and Regulation Act, (FCRA) 1976 as amended from time to time wherever applicable are adhered to strictly. They shall desist from opening accounts in the name of banned organizations and those without registration.

2.2 Designated Director:

Designated Director" means a person designated by the bank, to ensure overall KYC compliance with the obligations imposed under provisions of the PML Act and the Rules and includes a person duly authorized by the Board of Directors. The Designated Director is responsible for effective implementation of policies and procedures.

a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks.

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

2.3 Officially Valid Documents:

Officially Valid Document (OVD) means:

a. Proof of possession of Aadhaar Card/number
b. the Passport

c. the Driving License
d. the Voter Identity card issued by the Election Commission of India.
e. Job card issued by NREGA duly signed by an officer of State Government.
f. Letter Issued by the National Population Register containing details of name and address.

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

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

b. where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents there of shall be deemed to be OVDs for the limited purpose of proof of address:-
i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
ii. property or Municipal tax receipt;
iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation;

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

2.4 Principal Officer:

Principal Officer means an officer nominated by the bank under the Rule 8 of the PML Rules (Maintenance of Records who shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law and regulations.

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

2.4.1 - Digital KYC
Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorized officer of the RE as per the provisions contained in the Act.
2.4.2 – Digital Signature
Digital Signature" shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
2.4.3 Group" –
The term "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961. (43 of 1961)

2.4.4 Know Your Client (KYC) Identifier

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

2.5 Person:

In terms of PML Act a person includes

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

2.6 Transaction:

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

a. opening of an account
b. 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;
c. the use of a safety deposit box or any other form of safe deposit;
d. entering into any fiduciary relationship;
e. any payment made or received in whole or in part of any contractual or other legal obligation; or
f. Establishing or creating a legal person or legal arrangement.

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

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or

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

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

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

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

3.0 KEY ELEMENTS OF THE POLICY

The KYC Policy includes the following four key elements:

a. Customer Acceptance Policy (CAP);
b. Customer Identification Procedures (CIP)
c. Monitoring of Transactions; and
d. Risk Management

3.1 Customer Acceptance Policy (CAP)

Bank will develop clear customer acceptance policies and procedures, including a description of the types of customers that are likely to pose a higher than average risk to the Bank and including the following aspects of customer relationship in the Bank.

1. No account is opened or maintained in anonymous or fictitious/ benami name.
2. Bank will not open an account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and/ or obtain required documents either due to non-cooperation of the customer or non-reliability of the documents/ information furnished by the customer. Bank may also consider closing an existing account under similar circumstances.
3. No transaction or account based relationship is undertaken without following customer due diligence procedures.
4. The document and information either mandatory and/or optional/additional to be sought for KYC purpose while opening an account and during the periodic updation is specified.
5. Parameters of risk perception are clearly defined in terms of the nature of business activity, location of the customer and his clients, mode of payments, volume of turnover, social and financial status, etc. so as to enable the Bank in categorizing the customers into low, medium and high risk.
6. Circumstances, under which a customer is permitted to act on behalf of another person/ entity, shall be clearly spelt out in conformity with the established law and practice of banking.
7. Customer Due Diligence procedure is followed for all the joint account holders while opening a joint account
8. Since Customer Due Diligence procedure is followed at UCIC level, a KYC compliant customer of the bank shall not be required to have fresh Customer Due Diligence exercise.
9. Bank shall have suitable systems in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanction lists circulated by the Reserve Bank of India.
10. Customer Acceptance Policy shall not result in denial of banking / financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

3.1.1 Risk Perception in respect of Customer:

"Customer Risk" in the present context refers to the money laundering and terrorist funding risk associated with a particular customer from a Bank's perspective. This risk is based on risk perceptions associated with customer profile and level of risk associated with the product & channels used by Customer.

For categorising based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken – cash, cheque/monetary instruments, wire transfers, forex transactions, etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in

No bank or financial institutions are immune from internal and external frauds. Thus the level of Money Laundering Risk that Bank is exposed to by a customer relationship depends on following factors:

i. Type of the customer (constitution) and nature of business
ii. Type of product/ service availed by the customer
iii. Location / address of the customer, volume of business in the bank

Based on the above criteria, the customers are classified into three Risk levels, viz., High risk, Medium risk and low risk. ***The risk categorization of a customer and the specific reasons for such categorization shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer***.

Low Risk Customers : Individuals (other than High Net Worth) and entities, whose identity and source of income, can be easily identified, and customers in whose accounts the transactions conform to the known profile, may be categorized as low risk.

Medium Risk Customers: Customers that are likely to pose a higher than average risk to the bank should 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/her client profile, facilities or services enjoyed etc. Persons in business/industry or trading activity where the area of his/her residence or place of business has a scope or history of unlawful trading / business activity.

High Risk Customers: The branches may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

Various static and dynamic / financial parameters are defined on the basis of its experience as also the above factors, which are precisely mentioned in the 'risk matrix' as below.

The branches shall strictly adhere to Risk matrices and underlying guiding key notes in the process of risk categorization of its customers. The changes in the static parameters shall be initiated by the branches at the branch level and the dynamic / financial parameters shall be applied in the system software at periodic intervals. The entire process of customer risk categorization is semi-automatic (partially manual and partially automatic).

RISK MATRIX

STATIC PARAMETERS		
A	**B**	**C**
LOW RISK	**MEDIUM RISK**	**HIGH RISK**
Staff / Ex staff of the bank	Gas Station / Gas Agency	Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc.
Government and Semi Government employees and other salaried class customers whose salary structure is well defined.	Car/ Boat / Plane Dealership	Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of and for coping with terrorist activities.
Illiterates	Electronics (Wholesale)	Individuals and entities in watch list issued by Interpol and other similar international organisations.

Senior Citizens	Travel agency	Customers with dubious reputation as per public information available or commercially available watch lists.
Pensioner	Used car sales agencies/dealers	Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk.
Employees of Public sector undertakings	Tele-marketers	Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations etc.
Employees of Government / Semi government / Local body / Government departments / Government owned companies	Providers of telecommunications service, internet café, IDD call service, phone cards, phone centre	Politicians and their relatives, politically exposed persons (PEPs) etc
Employees of Regulators and Statutory bodies	Dot-com company or internet business	Non-resident and foreign nationals.
NPOs/ NGOs promoted by United Nations or its agencies	Pawn-shops/Pawn brokers	Non face-to-face customers.
Self Help Groups	Auctioneers	High net worth individuals (Refer Note # 5 below)
People belonging to low economic strata of the society whose accounts show small balances and low turnover (Refer Note #8 Below)	Cash Incentive Businesses such as Restaurants, retail shops, parking garages, fast food stores, movie theatres, etc.	Firms with 'sleeping partners'
Students / student support accounts	Sole Practioners or Law Firms (small, little known)	Companies having close family shareholding or beneficial ownership.
Social support accounts	Notaries (small, little known)	Complex business ownership structures, which can make it easier to

		conceal underlying beneficiaries, where there is no legitimate commercial rationale.
Individuals (other than those who are coming under Medium and High Risk category)	Secretarial Firms (small, little known)	Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local gent or low level staff does not constitute physical presence.
Employees of private sectors concerns.	Accountants (small, little known firms) like Chartered accountants, cost accountants, tax practitioners, company secretary, etc	Investment Management/ Money Management Company/ Personal Investment Company.
	Blind	Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc.
	Purdanashin woman	Trusts, Charities, NGOs/ NPOs (especially those operating on a "cross-border" basis) unregulated clubs and organisations receiving donations (excluding NPOs/ NGOs promoted by United Nations or its agencies), religious institutions.
	Stock brokerage agency / stock brokers	Gambling/ gaming including "Junket Operators" arranging gambling tours.
	Import/ Export agencies	Dealers in high value or precious goods (e g jewel, gem and precious metals dealers, art and antique dealers) and such other cash intensive business
	Proprietorship concerns	Customers engaged in a business which is associated with higher levels of corruption (eg: Arms manufacturers, dealers and intermediaries)
	Partnership concerns /	Customers that may

	LLP	appear to be Multi-level marketing companies etc.,
	Private Limited Companies / Public limited companies	Customers dealing in real estate and construction business
	Any Registered Bodies (other than those mentioned in Low risk and High risk category)	Associations and clubs
	Unregistered / unincorporated Associations / Body of Individuals	Foreign nationals / NRI
	Other corporate bodies	Bullion dealers and Jewelers (Dealers in Gems and Jewellers), Scrap dealers
	Agriculture activity	Non-Bank Financial Institution / Credit societies / Co-operative Societies
	Self-employed businessmen	HUF
	Employees of co-operative other societies and cooperative banks	Minor Accounts / Accounts operated by POA holders or Letter of Authority holders
		Executors/Administrators for the deceased accounts
		Accounts opened under / reference to Foreign Contribution Regulation Act for receiving foreign contributions
		Pooled Accounts maintained by professionals for their clients etc
		Customers located in border areas, criminal / terrorist outfit basis, centers of high risk business as identified by the bank from time to time
		Internet banking and other online banking facility (in case no limit is fixed for such online transactions)
		Accounts having Beneficial Owners.
		Autism, Cerebral palsy, mentally disabled persons

		Customers/accounts named in complaints (from legal enforcement authorities) or fraud is reported against the customer/account holder
DYNAMIC / FINANCIAL / ACCOUNTING PARAMETERS		
A	**B**	**C**
LOW RISK	**MEDIUM RISK**	**HIGH RISK**
-	-	Aggregate Balances in SB+CA+TD exceeding 1.00 crore on any day during the period for which the customer is subjected to review (i.e., review period 6 months as applicable for 'static parameters' under the said policy)
-	-	Aggregate credit limits / term loan facilities exceeding 2 crores on any day during the period for which the customer is subjected to review (i.e., review period 6 months as applicable for 'static parameters' under the said policy)
		Autism, Cerebral palsy, mentally disabled persons
-	-	Customer having any Account Inoperative, accounts shown in S T Reports (STR) and Cash Transaction Reports (CTR), accounts Frozen / blocked accounts, Customer accounts blocked or freezed on account of inadequate KYC, Court attached accounts, Unclaimed deposit accounts (deposits which are not claimed for more than 3 years), Customers whose accounts appear in Suspicious Transaction Alert Report and fulfils the conditions in Rule Violation Matrix (i.e., violation of transaction

		rules for no. of times specified in the rule violation matrix).
People belonging to Low income group (as defined in Note # 8)	-	High Net worth Individuals (as defined in Note # 5)
		Customers who have financial indiscipline in the bank as may be defined by the bank from time to time Eg: cheque returns in the customer accounts, Customers whose loan accounts are marked / categorized as NPA

Key Notes:

1. Branches shall prepare a Risk profile of each customer based on various information collected by them with regard to constitution of the customer, their nature of business, income level, place of residence (location of the customer), type of facilities enjoyed in the bank, etc (Static parameters) and the volume of business conducted in the bank (Financial / Dynamic parameters). The branch should apply enhanced due diligence measures in respect of High Risk customers.

2. Branches should apply 'KYC-updating exercise' to their existing clients at least every two years for High Risk customers, every eight years for Medium Risk customers and every ten years for Low Risk customers.

   Branches should also carry out '**ongoing due diligence'** of their existing clients in order to ensure that their transactions are consistent with the Bank's knowledge of the client, his business and risk profile and the source of funds and, if required, initiate necessary modification in the risk profile / risk category of such customers immediately, without waiting for the routine and periodical review procedure of the bank (i.e., once in every six months as mentioned in Note # 4 below).

3. System shall assign provisional risk categorization based on the system provided parameters. Branches shall review the same and make suitable modification/revision, if need be, based on remaining indicators / parameters as covered in the policy.

4. Customer Risk categorization and Profiling for **static parameters and dynamic/financial/accounting parameters** shall be reviewed by the branches once in every 6 months:

   For the period from April – September in the month of October
   For the period from October – March in the month of April

   The branches shall be responsible for submission of compliance report / certificate on KYC up-dation and risk profiling / risk categorization of their customers at such periodic intervals to the controlling office of the bank. Such compliance certificate / report shall

be subject to internal inspection / audit / verification procedure as may be laid down by the bank from time to time.

5. **High Net Worth Individuals means and include individuals whose**
   - Average Aggregate Balance in SB+CA+Term deposit exceeds 50 Lakh (based on six months average)

   or

   - the aggregate credit facilities / term loans availed exceeds 100.00 Lakh as on the last date of the month immediately preceding the month in which the review is conducted.

   'Term deposit' includes cash certificate, term deposits, recurring deposits, pigmy deposits, etc.
   'Matured deposits' shall be classified as demand deposits / CA

6. Risk Categorisation of customers and its review shall be based on combination of various parameters as mentioned in the matrix-table. Among the chosen parameters, highest risk grade will be assigned as overall Risk for the customer.
   For example: A Travel Agent (Medium risk) with Proprietorship account (medium risk) and having average aggregate balances in SB+CA+TD exceeding 1.00 crore (high risk), shall be assigned with overall rating of "High Risk".

7. At the time of opening the customer account, the risk categorisation shall be based on Static Parameters. The review / re-categorization shall be done on the basis of Financial / Dynamic parameters and Static Parameters taken together. During review, the risk assigned to an existing customer may undergo change depending on the change in risk parameters of the customer. Generally, the Financial / Dynamic parameters shall **override** the Static Parameters unless there is a substantial change in the Static parameters to be applied to a customer, which has the effect of increasing / decreasing the risk category of such customer as mentioned above.

8. **'Small Balance and low turnover accounts'** means such accounts in which the total credits during the year shall not exceed Rs. 1.00 Lakh and the total debits during a month shall not exceed Rs. 10,000.00 and the average monthly balance in such accounts does not exceed Rs. 50,000.00 (Based on previous 12 months information).

9. Student Support and Social Support Accounts will be always classified under low risks for the first six months and thereafter will depend on the dynamic / financial parameters.

10. The categorization of customers under risk perception is only illustrative and not exhaustive. The branches may categorize the customers according to the risk perceived by them while taking into account the above aspects. For instance, a salary class individual who is generally to be classified under low risk category may be classified otherwise based on the perception of the Branch/Office and based on following ***illustrative*** list of parameters, viz., unusual transaction / behaviour, submitted Suspicious Transaction Reports (STR) for staff-Customer. submitted Cash Transaction Report (CTR) for staff customer, frequent Cheque returns in the staff account etc.

11. Threshold limit for daily monitoring of transactions: Apart from the general parameters defined and applicable uniformly across all categories of customers, daily transactions alerts are defined in respect of each categories of customers based on the risk assigned to them as follows. Such transactions alerts are to be checked and verified by the branch

head (at the branch level) and simultaneously monitored by the AML department at the central office on daily basis.

Type of customers	Threshold limit per transaction in any account
Low risk customer	5.00 Lakh per transaction
Medium risk customer	3.00 Lakh per transaction
High risk customer	2.00 Lakh per transaction

3.2 Customer Identification Procedure (CIP)

1. General

a. Customer identification means undertaking client due diligence measures while commencing an account-based relationship including identifying and verifying the customer and the beneficial owner on the basis of one of the documents proving their identity. Bank will also obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of banking relationship. The Bank shall observe client due diligence based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based approach is necessary to avoid disproportionate cost to the bank and a burden- some regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc.).

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

i. while establishing a banking relationship;

ii. while carrying out a financial transaction;

iii. when the Bank has a doubt about the authenticity or adequacy of the customer identification data it has obtained;

iv. when bank sells third party products as agent;

v. while selling Bank's own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than Rs. 50,000.00

vi. when carrying out transactions for a non-account based customer, that is a walk-in- customer, where the amount is equal to or exceeds Rs. 50,000.00 whether conducted as a single transaction or several transactions that appear to be connected;

vii. when the Bank has reason to believe that a customer (account based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000.00

'Mandatory' information required for KYC purpose which the customer is obliged to give while opening an account should be obtained at the time of opening the account/ during periodic updation. Other 'optional' customer details/additional information, if required may be obtained separately after the account is opened

only with the explicit consent of the customer.

c. **While undertaking customer identification, bank shall ensure that:**

i. Decision-making functions of determining compliance with KYC norms shall not be outsourced

ii. Introduction shall not be sought while opening accounts.

iii. The customers shall not be required to furnish an additional OVD, if the OVD submitted by the customer for KYC contains both proof of identity and proof of address.

iv. The first requirement of knowing your customer for anti-money laundering purposes is to be satisfied about the identity of the person who claims to be a prospective customer.

v. The second requirement of knowing the customer is to ensure that sufficient information is obtained on the nature of the business that the customer expects to undertake or any expected, or predictable pattern of transaction.

vi. Verification of identity means, it has been decided by the Reserve Bank that 'simplified measures' may be applied in the case of 'Low Risk' customer taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering the terrorist financing risks involved.

vii. Customer categorized as low risks expresses inability to complete the documentation requirement on account of any reason that the bank considers genuine and where it is essential not to interrupt the normal conduct of business, the regulator may permit the reporting entity to complete the verification within a period of 6 months from the date of establishment of relationship.

2. Customer Due Diligence requirements

I. CDD while opening accounts

A. Accounts of individuals:

a. For opening accounts of individuals who are eligible for enrolment of Aadhaar, branches shall obtain the following:

i. Aadhaar Number (Copy of Aadhaar Card) which serves as both a proof of Identity and address. Further, where an Aadhaar Number is not assigned to an individual, proof of application of enrolment for Aadhaar which is not older than 6 months.

ii. Permanent Account Number (PAN) or Form 60 as defined under Income Tax Rules 1962, as amended from time to time. Further, where a PAN is not submitted, certified copy of OVD containing details of identity and address is to be submitted.

iii. One recent photograph

b. For opening accounts of individuals who are residents of state of J & K, Assam or Meghalaya, who do not submit Aadhaar or proof of application of enrolment for Aadhaar, branches shall obtain the following:

i. Certified copy of OVD containing details of identity and address is to be submitted.

ii. One recent photograph

c. For opening accounts of individuals who are not eligible for enrolment of Aadhaar, branches shall obtain the following:

i. Permanent Account Number (PAN) or Form 60 as defined under Income Tax Rules 1962, as amended from time to time.
ii. Certified copy of OVD containing details of identity and address is to be submitted.
iii. One recent photograph
iv. A declaration to the effect of individual not being eligible for enrolment for Aadhaar.

While opening account of legal entities apart from obtaining documents pertaining to such entities, documents pertaining to individuals who are beneficial owners, authorized signatory or power of attorney holder of such legal entity shall be obtained as per the above criteria.

d. In case the identity information relating to Aadhaar or PAN submitted by the customer does not have the current address of the customer, an official valid document as defined under Clause No.2.3 shall be obtained from the customer for this purpose.

Provided further that where 'simplified measures' are applied for verifying, for the limited purpose of, proof of address the following additional documents are deemed to be OVDs:

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

The customer shall submit Aadhaar or OVD updated with current address within a period of three months of submitting the above documents.

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

b. **e-KYC services of UIDAI:**

In order to reduce the risk of identity fraud, document forgery and to have paperless KYC verification, UIDAI has launched its e-KYC service. The Reserve Bank of India has directed the banks to accept e-KYC service as a valid process for KYC verification under Prevention of Money Laundering (Maintenance of Records) Rules, 2005. Further, the information containing demographic details and photographs made available from UIDAI as a result of e-KYC process (which is in an electronic form and accessible so as to be usable for a subsequent reference) shall be treated as an "Officially Valid Document" under PML Rules. While using e-KYC service of UIDAI, the individual user (i.e. prospective customer) has to authorize the UIDAI, by explicit consent, to release his/ her identity/ address

through biometric authentication to the Bank branches. The UIDAI then transfers the data of the individual comprising name, age, gender and photograph of the individual, electronically to the Bank, which may be accepted as valid process for KYC verification. Branches shall accept e-Aadhaar downloaded from UIDAI website as an "Officially Valid Document" subject to the following:

i. If the prospective customer knows only his/ her Aadhaar number, the branch shall print the prospective customer's e-Aadhaar letter directly from the UIDAI portal; or adopt e-KYC procedure
ii. If the prospective customer carries a copy of the e-Aadhaar downloaded from a place/source elsewhere, still the branch shall print the prospective customer's e-Aadhaar letter directly from the UIDAI portal; or adopt e-KYC procedure; or confirm the identity and address of the resident through the authentication service of UIDAI. Physical Aadhaar card/letter issued by UIDAI containing details of name, address and Aadhaar number received through post and e-KYC process mentioned under "Operational Procedure" would continue to be accepted as an "Officially Valid Document".
iii. In case the customer fails to submit the Aadhaar or PAN/ Form 60 within a period of 6 months period, the said account shall cease to be operational till the time the Aadhaar Number and PAN/ Form 60 is submitted by the customer. The customers will be informed about this provision at the time of opening of the account.

iv) The KYC Identifier with an explicit consent to download records from CKYCR

c. **Introduction of accounts**:

Since introduction from an existing customer is not necessary for opening accounts under PML Act and Rules or the RBI's extant instructions, branches shall not insist on introduction for opening of bank accounts. After passing of PML Act and introduction of document based verification of identity/ address of the proposed account holders, the accounts opened with proper documents are considered as acting in good faith and without negligence by the banks.

d. **Simplified Measures for proof of identity**

If an individual customer does not have any of the OVDs (as mentioned in para 2.3 as proof of identity, then 'simplified measures' shall be applied in the case of 'Low risk' customers taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved. Accordingly, in respect of low risk category of customers, where simplified measures are applied, it would be sufficient to obtain any one of the documents referred under para 2.3 (i), which will be deemed as an OVD for the purpose of proof of identity.

e. **Simplified Measures for Proof of Address**

The additional documents mentioned under para 2.A.d shall be deemed to be OVDs under "simplified measure" for the low risk customers for the limited purpose of **proof of address** where customers are unable to produce any OVD for the same.

f. **Accounts of married woman**

As per the amendment to the Rules, 2005 (Gazette notification dated 22.09.2015), a document shall be deemed to an "officially valid document" even if there is a change in the name subsequent to its issuance, provided it is supported by a marriage certificate issued by the State Government or a Gazette notification, indicating such a change of name. Accordingly, Branches shall accept a copy of

marriage certificate issued by the State Government or Gazette notification indicating change in name, together with a certified copy of the 'officially valid document' in the existing name of the person while establishing an account based relationship or while undergoing periodic updation exercise.

g. Small Accounts

It has been observed that a large number of persons, especially, those belonging to low income group both in urban and rural areas are not able to produce such documents to satisfy the Bank about their identity and address. This would lead to their inability to access the banking services and result in their financial exclusion. In such cases, if a person who wants to open an account and is not able to produce any of the OVDs or the documents applicable in respect of simplified procedure, bank shall open a "small account". The small accounts can be opened under Savings Bank Deposit Account. The features of the above account and restrictions stipulated by RBI/Govt. of India are as follows:

i. Accounts where aggregate of all credits in a financial year does not exceed Rs.1.00 Lakh
ii. Accounts the aggregate of all withdrawals and transfers in a month does not exceed Rs.10,000 and
iii. Where the balance at any point of time does not exceed Rs.50,000

Any violation of the stipulations mentioned above will result in restraining the operations in the account after giving due notice to the account holder.

Small Savings Bank Deposit account can be opened on production of a self attested photograph and affixation of signature or thumb impression as the case may be, on the form for opening the account, provided that the designated bank official while opening the account certifies under his signature that the person opening the account has affixed his signature or thumb impression as the case may be, in his presence.

A Small Savings Bank Deposit Account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the Bank of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months.

A Small Savings Bank Deposit Account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of customer shall be established through the production of officially valid documents.

Foreign remittances shall not be allowed to be credited into a Small Savings Bank Deposit Account unless the identity of the customer is fully established through the production of officially valid documents

h. **Basic Savings Bank Deposit Accounts**

The "Basic Savings Bank Deposit Account" shall offer following minimum common facilities to all the customers:

i. The basic Savings Bank Deposit Account shall be considered a normal banking service available to all.
ii. This account shall not have the requirement of any minimum balance.

iii. The service available in the account will include deposit and withdrawal of cash at bank branch as well as ATMs; receipt/credit of money through electronic payment channels or by means of deposit/ collection of cheques drawn by Central/ State Government agencies and departments.

iv. While there will be no limit on the number of deposits that can be made in a month, account holders will be allowed a maximum of four withdrawals in a month, including ATM withdrawals; and
v. Facility of ATM Card or ATM-cum-Debit Card

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

The Basic Savings Bank deposit Account would be subject to RBI instructions on Know Your Customer (KYC)/ Anti-Money laundering (AML) for opening of bank accounts issued from time to time. If such account is opened on the basis of simplified KYC norms, the account would additionally be treated as a "Small Account" and would be subject to conditions stipulated for such accounts as detailed for such accounts

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

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

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

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

i. letter, cheque books, ATM cards;

ii. telephonic conversation;

iii. Visits; etc.,

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

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

l. In case of close relatives, e.g. husband, wife, son, daughter and parents etc. who live with their wife, husband, father/ mother, daughter and son, who do not have officially valid document for address verification, then, in such cases, branches should obtain an OVD for proof of address and identity of the relative with whom the prospective customer is living, together with a declaration from the relative that the said person (prospective customer) proposing to open an account is a relative and is staying with him/her.

m. Branches are not required to obtain fresh documents of customers when customers approach them for transferring their account from one branch of the Bank to another branch. KYC once done by one branch of the Bank shall be valid for transfer of the account within the Bank if full KYC verification has been done for the concerned account and is not due for periodic updation. The customer shall

be allowed to transfer his account from one branch to another branch without restrictions. Branches may transfer existing accounts at the transferor branch to the transferee branch without insisting on fresh proof of address and on the basis of a self declaration from the account holder about his/her current address. If an existing KYC compliant customer of the Bank desires to open another account in the Bank, there should be no need for submission of fresh proof of identity and/or proof of address for the purpose.

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

o. For the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship, the branch may rely on a third party; subject to the conditions that-

i. the branch immediately obtains necessary information of such client due diligence carried out by the third party;

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

iii. the branch is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act;

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

v. The branch is ultimately responsible for client due diligence and undertaking enhanced due diligence measures as applicable.

p. **Accounts of non-face-to-face customers**

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

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

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

close relatives of PEPs. The decision to open an account of a PEP as well as the decision to continue the business relationship in the event of an existing customer or relatives of an existing customer subsequently becoming a Politically Exposed Person (PEP), has to be taken by branch managers only.
In the event of an existing customer or the beneficial owner of an existing account subsequently becoming PEP, the account shall be subjected to the Customer Due Diligence (CDD) measures as applicable to PEPs including enhanced monitoring on an ongoing basis. PEPs, customers who are close relatives of PEPs and accounts where PEP is the ultimate beneficial owner shall be categorized 'high risk' so that appropriate transaction alerts are generated and the accounts are subjected to enhanced CDD on an ongoing basis.
Bank shall have appropriate ongoing risk management systems for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner.

B. Accounts of persons other than individuals

a. Accounts of Companies:

Where the customer is a company, one certified copy each of the documents mentioned here under are to be obtained for customer identification.

i. Certificate of incorporation

Ii Memorandum and Articles of Association;

iii. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and
iv. An officially valid KYC document in respect of managers, officers or employees holding an attorney to transact on its behalf.
v. PAN number of the Company
vi. Documents, as specified in Section 16, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.
vii. the names of the relevant persons holding senior management position
vii. the registered office and the principal place of its business, if it is different

Bank need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. Bank shall examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

b. **Accounts of Partnership firms:**

Where the customer is a partnership firm, one certified copy each of the documents mentioned here under obtained for identification

i. Registration certificate

ii. Partnership deed

iii. An officially valid KYC document in respect of the person holding an attorney to transact on its behalf
iv. PAN number of the **Partnership firms.**
v. ***Documents, as specified in Section 16, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to***

transact on the company's behalf.
vi. Names of all the partners
vi. The registered office and the principal place of its business, if it is different.

c. **Accounts of Trusts:**

Where the customer is a Trust, one certified copy each of the documents mentioned under Annexure-I are to be obtained for customer identification.

i. Registration certificate

ii. Trust deed

iii. An officially valid KYC document in respect of the person holding an attorney to transact on its behalf

iv. ***Permanent Account Number or Form No.60 of the trust.***
vi. Documents, as specified in Section 16, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.
vii. The names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust.
viii. The address of the registered office of the trust.
viii. list of trustees and documents, as specified in Section 16, for those discharging the role as trustee and authorized to transact on behalf of the trust

d. **Accounts of Unincorporated association or a body of individuals:**

Where the customer is an unincorporated association or body of individuals, one certified copy each of the documents mentioned here under are to be obtained for customer identification.

i. Resolution of the managing body of such association or body of individuals

ii. Power of attorney granted to the persons authorized to transact on its behalf

iii. An officially valid document in respect of the person holding an attorney to transact on its behalf; and

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

v. ***Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals.***
vi. Documents, as specified in Section 16, relating to beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.
vii. Such information as may be required by the RE to collectively establish the legal existence of such an association or body of individuals.
Explanation: Unregistered trusts/partnership firms shall be included under the term 'unincorporated association'.
Explanation: Term 'body of individuals' includes societies.

e. **Accounts of Proprietary Concerns:**

For proprietary concerns, in addition to the OVD applicable to the individual (proprietor), any two of the following documents in the name of the proprietary concern are required to be submitted:

i. Registration Certificate

ii. Certificate/ License issued by the Municipal Authorities under Shop and Establishment Act
iii. Sales and Income Tax Returns

iv. CST/VAT/GST Certificate (Provisional/Final)

v. Certificate/Registration document issued by Sales Tax/ Service tax/ Professional Tax authorities
vi. IEC (Import Export Code) issued to the proprietary concern by the office of DFGT or License/ Certificate of practice in the name of the proprietary concern by any professional body incorporated under a statute
vii The complete Income Tax return (not just the acknowledgement) in the name of the sole Proprietor where the firm's income is reflected duly authenticated/ acknowledged by the Income Tax Authorities.
viii. Utility bills such as electricity, water and landline telephone bills

Though the default rule is that any two documents mentioned above should be provided as activity proof by a Proprietary concern, in cases where the branches are satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof.
In such cases, the branches, however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern.

f. **Client accounts opened by professional intermediaries**:

i. When the Bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client shall be identified.
ii. Bank may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
iii. Branches shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Bank.
iv. Where funds held by the intermediaries are not co-mingled at the Bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners shall be identified.
v. Where such funds are co-mingled at the Bank, the Bank shall still look into the beneficial owners. Where the Bank rely on the 'customer due diligence' (CDD) done by an intermediary, Bank shall satisfy itself that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers.
vi. The ultimate responsibility for knowing the customer lies with the Bank.

C. Beneficial Ownership

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

conducted, and includes a person who exercises ultimate effective control over a juridical person.

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

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

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

Explanation.- For the purpose of this sub-clause-

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

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

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

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

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

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

vi. Where the client or the owner of the controlling interest is a **company listed on a stock exchange**, or is a subsidiary of such a company**,** it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies. There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. In such cases, Bank shall determine whether the customer is acting on behalf of another person as trustee/ nominee or any other intermediary. If so, Bank shall insist on satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. The different categories of beneficiaries should be identified as defined above. In the case of a 'foundation', steps shall be taken to verify the founder managers/directors and the beneficiaries, if defined.

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

Explanation- For the purpose of this sub-clause.
1."Controlling ownership interest" means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.
2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

b. Where the customer is a partnership firm, the beneficial owner is the Natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10percent of capital or profits of the partnership or who exercises control through other means.
Explanation - For the purpose of this sub-clause, "control" shall include the right to control the management or policy decision.

c. Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent of the property orcapital or profits of the unincorporated association or body of individuals.
Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10 percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through achaing of control or ownership.
"Certified Copy" - Obtaining a certified copy by the bank shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the bank as per the provisions contained in the Act.

D. **Accounts of Non Profit Organizations**

A Non Profit Organization (NPO) means any entity or organization that is registered as a Trust or a Society under the Societies Registration Act, 1860 or any similar State Legislation or a company registered under Section 25 of the Companies Act 1956. All transactions involving receipts by these NPOs of value more than Rs.10 Lakh or its equivalent in foreign currency is to be reported to FIU-IND centrally from Head Office. However, if the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 10 Lakh the Bank shall consider filing a Suspicious Transaction Report to FIU-IND undertaken and the adequacy of data obtained. Full

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

E. **Accounts operated by Power of Attorney Holders/Letter of Authority Holders:**

In case of accounts operated by Power of Attorney (POA) Holders / Letter of Authority (LOA) Holders, KYC documents shall be obtained from such POA holders/ LOA holders and records shall be maintained/ updated in the system**.**

II. **Introduction of New Technologies - debit cards etc.,**

Bank will pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent the same being used for money laundering purposes. The Electronic Cards (debit card, etc.) issued by the Bank to the customers may be used by them for buying goods and services, drawing cash from ATMs and electronic transfer of funds. Bank shall ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. Bank shall ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also.

F. On-going Due Diligence

i. Bank will undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers'

Business and risk profile, the source of funds / wealth.

ii. 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.

For ongoing due diligence, REs may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

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

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

(a) A system of periodic review of risk categorization 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.

III. Periodic updation of KYC

A. CDD requirements for periodic updation:

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

i. Branches should apply client due diligence measures/full KYC exercise to existing clients at least every two years for high risk customers, every eight years for medium risk customers and every ten years for low risk customers taking into account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained.
   Full KYC exercise may include all measures for confirming identity and address and other particulars of the customer that the Bank may consider reasonable and necessary based on the risk profile of the customer. The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.
   Branches should carry out ongoing due diligence of existing clients in order to ensure that their transactions are consistent with the Bank's knowledge of the client, his business and risk profile and where necessary, the source of funds.
   Branches should undertake client due diligence measures while commencing an account-based relationship. Such measures include identifying and verifying the customer and beneficial owner on the basis of reliable and independent information and data or documentation**.**
   The periodical verification/updation of customer data shall be done irrespective of whether the account has been transferred from one branch to another and Bank shall maintain records of transactions as prescribed.
   Branches other than Home (Base) Branch shall perform Full KYC exercise/ Positive confirmation, whenever the customer approaches that branch and requests the branch to complete the Full KYC exercise/Positive confirmation by submitting the required documents. Such branches should exercise due diligence in verification of the documents and updation of the details in the CBS system.
ii. Branches need not seek fresh proofs of identity and address at the time of periodic updation from those customers who are categorized as 'low risk', in case of no change in status with respect to their identities and addresses. A self certification by the customer to that effect should suffice in such cases. In case of change of address of such 'low risk' customers, they could merely forward a certified copy of the document (proof of address) by mail/post, etc. Branches need not insist on physical presence of such low risk customer at the time of periodic updation.
iii. Fresh photographs and Officially Valid Documents shall be obtained from minor customer on becoming major

B Freezing and Closure of accounts

It would always be open to the Bank to close the account of KYC non-compliant customers after issuing due notice to the customer explaining the reasons for

taking such a decision. Such decisions need to be taken by the Branch Manager.

While it is absolutely necessary for banks as well as customers to comply with the measures prescribed for KYC/AML purposes, drastic measures like closing of accounts may be taken only after sending out sufficient discernible warning signals to the customers, basing on the level of customer education and public awareness on the subject. In all such cases where the account holders are either not responding over a period of time/not found at the given address, Bank may take such action as deemed necessary to comply with KYC/AML guidelines without denying basic banking facilities.

Before taking the extreme step of closing an account on account of non compliance with the KYC/AML requirements, as an initial measure, branches are advised to place such accounts under close watch, depriving the non-compliant customers certain additional facilities, till the customer complies with such requirements.

This exercise, however, should not extend beyond a period of three months. If the customer despite such measures, shows unwillingness to comply with KYC/AML/ CFT requirements, branches would be free to proceed further and close the accounts after giving due notice to him/her. It is reiterated that basic banking transactions already in force should not be disturbed for meeting KYC review requirements.

In case of non-compliance of KYC requirements by the customers despite repeated reminders by branches, branches should impose "partial freezing" on such KYC non-compliant in a phased manner. Meanwhile, the account holders can revive accounts by submitting the KYC documents as per instructions in force. While imposing "partial freezing", branches are advised to ensure that the option of 'partial freezing' is exercised after giving due notice of three months initially to the customers to comply with KYC requirements and followed by a reminder for further period of three months. Thereafter, branches to impose "partial freezing" by allowing all credits and disallowing all debits with the freedom to close the accounts**.**

If the accounts are still KYC non-compliant after six months of imposing initial "partial freezing", branches should disallow all debits and credits from/to the accounts, rendering them inoperative.

Further, it would always be open to the branches to close the account of such customers after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions, however, need to be taken by the Branch Manager.

In the Circumstances when the Bank believes that it would no longer be satisfied about the true identity of the account holder, the Bank shall file a Suspicious Transaction Report (STR) with Financial Intelligence Unit India (FIU-IND) under the Department of Revenue, Ministry of Finance, Government of India

IV. Miscellaneous

A. Operation of Bank Accounts & Money Mules

Money mules are individuals with bank accounts who are recruited by fraudsters to receive cheque deposit or wire transfer for the purpose of money laundering. "Money Mules" can be used to launder the proceeds of fraud schemes (*e.g.,* phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "money mules." In order to minimize the operations of such mule accounts, Branches should strictly adhere to the guidelines on opening of accounts and monitoring of transactions.

B. Simplified norms for Self Help Groups (SHGs):

i. In order to address the difficulties faced by Self Help Groups (SHGs) in complying with KYC norms wile opening Savings Bank accounts and credit linking of their accounts, following simplified norms shall be followed by branches:

ii. KYC verification of all the members of SHGs need not be done while opening the Savings Bank account of the SHGs and KYC verification of all the office bearers would suffice.

As regards KYC verification at the time of credit linking of SHGs, no separate KYC verification of the members or office bearers is necessary.

C. Walk in Customers

In case of transactions carried out by a non-account based customer, that is a walk-in customer, where the amount of transaction is equal to or exceeds Rs.50000, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address shall be verified.

If the Bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50000, the Bank shall verify identity and address of the customer and also consider filing a Suspicious Transaction Report to FIU-IND. The identity and address of the Walk-in customer shall be verified by obtaining KYC documents and records are to be maintained/ updated in the system**.** Bank shall also verify the identity of the customers for all international money transfer operations.

D. Issue of Demand Drafts, etc., for more than Rs. 50000

Any remittance of funds by way of Demand Draft, mail/telegraphic transfer or any other mode for value of Rs. 50000 and above shall be effected by debit to the customer's account or against cheques and not against cash payment. Bank shall not make payment of cheques/ drafts/pay orders/banker's cheques if they are presented beyond the period of three months from the date of such instrument.

E. Unique Customer Identification Code (UCIC)

A Unique Customer Identification Code (UCIC) will help the Bank to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable the Bank to have a better approach to risk profiling of customers. Branches are required to strictly avoid creating multiple customer IDs while opening new accounts and in case of existing multiple IDs, branches have to carry out the process of de-duplication

3.3 Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC/AML procedures. Branches should exercise ongoing due diligence with respect to every customer and closely examine the transactions to ensure that they are consistent with the customer's profile and source of funds as per extant instructions. The ongoing due diligence may be based on the following principles

1. The extent of monitoring will depend on the risk category of the account. High risk accounts have to be subjected to more intensified monitoring.
2. Branches should pay particular attention to the following types of transactions:

i. Large and complex transactions and those with unusual patterns, which have no apparent economic rationale or legitimate purpose.
ii. Transactions which exceed the thresholds prescribed for specific categories of accounts.
iii. Transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer.
iv. High account turnover inconsistent with the size of the balance maintained

3. Bank shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorization of customers shall be carried out at a periodicity of not less than once in six months.
4. Branches should closely monitor the transactions and analyze data in cases where a large number of cheque books are sought; there are multiple small deposits (generally in cash) across the country in one bank account and where a large number of cheques are issued bearing similar amounts/dates. Where such features are noticed by the branches and in case they find such unusual operations in their accounts, the matter should be immediately reported to Reserve Bank and other appropriate authorities such as FIU-IND.
5. Supervisors should keep a vigil over the transactions involving huge amounts. Transactions should generally have a bearing with the occupation and /or line of business of the account holders. In case of any doubt necessary enquiries shall be made with the account holders.
6. While accepting the cheque for collection, it is to be ensured that the name mentioned in the chalan and name of the beneficiary of the instrument are same.
7. Branches are advised to mandatorily obtain either PAN or Form 60/61 (if PAN is not available) for opening of accounts and also at the time of accepting cash receipt for Rs.50000 and above. If the customer appears to be structuring the transactions into a serious of transactions below the threshold of Rs.50,000 branches are required to obtain PAN or Form 60/61 (if PAN is not available) from the customer. Branches are advised to aggregate the split transactions across accounts of same customer to decide on the matter of obtention of PAN or Form 60/61, wherever the aggregate amount of transactions is Rs.50000 and above.
8. All the staff members are instructed to maintain the standards of good conduct and behaviour expected of them and not to involve in any activity that would bring disrepute to the institution and not to advise potential customers on the lines that would be an infringement of the legal process/ could facilitate money laundering/ could defeat the KYC norms or the norms of due diligence prescribed by RBI from time to time.

3.4 Risk Management

1. The inadequacy or absence of KYC standards can subject the Bank to serious customer and counter party risks especially reputational, operational, legal and concentration risks. Reputational Risk is defined as the potential that adverse publicity regarding the Bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution

2. Operational Risk can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Legal Risk is the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of the Bank. Concentration Risk although mostly applicable on the assets side of the balance sheet, may affect the liabilities side as it is also closely

associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the Bank's liquidity. It is worth noting that all these risks are interrelated. Any one of them can result in significant financial cost to the Bank as well as the need to divert considerable management time and energy to resolve problems that arise.

3. Customers frequently have multiple accounts with the Bank, but in offices located at different places. To effectively manage the reputational, operational and legal risk arising from such accounts, Bank shall aggregate and monitor significant balances and activity in these accounts on a fully consolidated basis, whether the accounts are held as on balance sheet, off balance sheet or as assets under management or on a fiduciary basis.

4. Branches should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge about the clients, their business and risk profile and where necessary, the source of funds. The Board of Directors of the Bank shall ensure that an effective KYC AML/CFT programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It shall cover proper management oversight, systems and controls, segregation of duties, training of staff and other related matters.

5. In addition, the following also to be ensured for effectively implementing the AML/CFT requirements:
   i. Allocation of responsibility for effective implementation of policies and procedures.
   ii. Independent evaluation by the compliance functions of Bank's policies and procedures, including legal and regulatory requirements.
   iii. Concurrent/ internal audit to verify the compliance with KYC/AML policies and procedures.
   iv. Putting up consolidated note on such audits and compliance to the Audit Committee at quarterly intervals.

6. Bank shall prepare a profile for each new customer based on risk categorization. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the bank.

7. Bank shall categorize its customers into low, medium and high risk category based on the assessment and risk perception of the customers, identifying transactions that fall outside the regular pattern of activity and not merely based on any group or class they belong to. The Bank shall have a Board approved policy for risk categorization and ensure that the same is meticulously complied with, to effectively help in combating money laundering activities. The nature and extent of due diligence, shall be based on the following principles:
   i. Individuals (other than High Net Worth) and entities, whose identity and source of income, can be easily identified, and customers in whose accounts the transactions conform to the known profile, shall be categorized as low risk.
   Illustrative examples include salaried employees and pensioners, people belonging to lower economic strata, government departments and government owned companies, regulators and statutory bodies, etc.

ii. Customers who are likely to pose a higher than average risk shall be categorized as medium or high risk depending on the background, nature and location of activity, country of origin, sources of funds, customer profile, etc. Customers requiring very high level of monitoring, e.g., those involved in cash intensive business, Politically Exposed Persons (PEPs) of foreign origin, shall be categorized as high risk.

8. Whenever there are suspicions of money laundering or financing of activities relating to terrorism or where there are doubts about the veracity of previously obtained customer identification data, branches should review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of business relationship.

4.0 Wire Transfers

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

1. Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. The originator and the beneficiary may be the same person.
2. Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institutions are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.
3. Domestic wire transfer means any wire transfer where the originator and receiver are located in the same country. It may also include a chain of wire transfers that takes place entirely within the borders of a single country even though the system used to effect the wire transfer may be located in another country.
4. The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the bank to perform the wire transfer.
5. Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and / or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analyzing suspicious or unusual activity and disseminating it as necessary.

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

   i. **Cross-border wire transfers**

      The bank does not conduct cross border wire transfers

ii. **Domestic wire transfers**

a. Information accompanying all domestic wire transfers of Rs. 50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.

b. If the Bank has reason to believe that a customer is intentionally structuring wire transfers to below Rs. 50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the Bank shall insist on complete customer identification before effecting the transfer. In case of non-co-operation from the customer, efforts shall be made to establish his identity and Suspicious Transaction Report (STR) shall be made to FIU-IND.

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

iii. Exemptions

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

iv. The role of Ordering, Intermediary and Beneficiary Banks

a. Ordering Bank

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

b. Intermediary bank

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

c. Beneficiary Bank

A Beneficiary Bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they should be reported to the Financial Intelligence Unit-India. As Beneficiary Bank, the Bank

shall also take up the matter with the Ordering Bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information on the remitter, the Bank shall consider restricting or even terminating its business relationship with the Ordering Bank.

5.0 Maintenance of KYC Documents and Preservation period

PML Act and Rules cast certain obligations on the banks with regard to maintenance, preservation and reporting of customer account information. Bank shall take all steps considered necessary to ensure compliance with the requirements of the Act and Rules.

5.1 Maintenance of records of transactions

Bank shall have a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005), as mentioned below:

1. all cash transactions of the value of more than Rs.10.00 Lakh or its equivalent in foreign currency;
2. series of all cash transactions integrally connected to each other which have been individually valued below Rs.10.00 Lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of Rs.10.00 or its equivalent in foreign currency
3. all transactions involving receipts by non-profit organizations of value more than Rs.10.00 Lakh or its equivalent in foreign currency
4. all cash transactions were forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;
5. all suspicious transactions whether or not made in cash and by way of

    i. deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of;
        a. cheques including third party cheques, pay orders, demand drafts, or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or
        b. transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts or
        c. any other mode in whatsoever name it is referred to;

    ii. credits or debits into and from any non-monetary accounts such as Demat Account, Security Account in any currency maintained by the bank, financial institution and intermediary, as the case may be ;

    iii. money transfer or remittances in favour of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transaction on its own account in any currency by any of the following (a) Cashier's Cheques, (b) Demand Drafts, (c) Wire or electronic remittances or transfers, (d) Internet transfers, (e) Automated Clearing House remittances, (f) Remittance for cards, (g)
    Any other mode of money transfers by whatever name called

    iv. Loans and advances including credit or loan substitutes, investments and contingent liabilities by way of:

a. subscription to debt instruments such as commercial papers, certificate of deposits, preference shares, debentures, securitized papers, interbank participation or any other investment in securities or the like in whatever form and name it is referred to
b. purchase and negotiation of bills; cheques and other instruments, or
c. letter of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/ or credit support
d. collection services by way of collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to.

6. All wire transfers of value more than Rs.5.00 Lakh.

7. All purchase and sale by any person, of immovable property valued at Rs.50.00 Lakh or more that is registered by the bank, as the case may be.
8. Bank shall maintain all necessary information in respect of transactions prescribed under Rule 3 of PML Rules, 2005 so as to permit reconstruction of individual transactions, including the following information:
   a. the nature of the transactions;
   b. the amount of the transaction and the currency in which it was denominated;
   c. the date on which the transaction was conducted; and
   d. the parties to the transaction

5.2 Preservation of Records

Bank shall take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.
The following steps shall be taken regarding maintenance, preservation and reporting of customer account information with reference to provisions of PML Act and Rules. Bank shall,

1. Maintain all necessary records of transactions between the Bank and the customer, both domestic and international, for at least five years from the date of transaction
2. 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 ;
3. Make available the identification records and transaction data to the competent authorities upon request ;
4. 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) ;
5. 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.

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

7. As per RBI circular UBD BPD (PCB) MC No. 16/12.05.001/ 2014-15 dated July 01, 2014, for the following transactions, proper records are to be maintained :
   i. All cash transactions of the value of more than Rupees Rs.10.00 Lakh or its equivalent in foreign currency.
   ii. All series of cash transactions integrally connected to each other which have been valued below Rs.10.00 Lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rs.10.00 Lakh,
   iii. All cash transactions, where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transaction and,

8. Bank shall pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background, including all documents / office records / memorandums pertaining to such transactions and purpose thereof shall, as far as possible, be examined and the findings, at branch as well as Principal Officer level, shall be properly recorded. Such records and related documents shall be made available to help auditors to scrutinize the transactions and also to Reserve Bank / other relevant authorities. These records will be preserved for five years as is required under PMLA, 2002.

6.0 COMBATING FINANCING OF TERRORISM (CFT)

6.1 The United Nations periodically circulates the following two lists of individuals and entities, suspected of having terrorist links, and as approved by its Security Council (UNSC):

1. (a) The ISIL (Da'esh) & Al-Qaida Sanctions List includes names of individuals, groups, undertakings and entities associated with the ISIL (Da'esh)/ Al-Qaida. The updated ISIL (Da'esh)/ Al-Qaida Sanctions List is available at http:// www.un.org/sc/ committees/ 1267/ aq_sanctions_list.shtml..
2. 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 Http://www.un.org/sc/committees/ 1988/list.shtml.
3. The United Nations Security Council Resolutions (UNSCRs), received from Government of India, are circulated by the Reserve Bank to all banks and FIs. Bank shall update the lists and take them into account for implementation of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, as detailed under para 6.2.
4. Branches are required to screen customer names with UN List of terrorist individuals/ entities before creation of new customer ID/opening of accounts. Branches are required to ensure that the names/s of the proposed customer does not match with that of the UN list of Terrorist individuals/organization/ entities, before opening any new account. Branches are also required to cross check the details of all existing accounts with the updated list and ensure that no account is held by or linked to any of the entities or individuals included in the list maintained for this purpose. If the particulars of any of the account/s have resemblance with those appearing in the list, branches have to verify transactions

carried out in such accounts and report those accounts to RBI/Financial Intelligence Unit-INDIA, New Delhi.

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

1. The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has issued an Order dated August 27, 2009 detailing the procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 for prevention of, and for coping with terrorist activities. In terms of Section 51A, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by on behalf of or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism and prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

2. Bank shall strictly follow the procedure laid down in the UAPA Order dated August 27, 2009 and ensure meticulous compliance to the Order issued by the Government.

6.3 Jurisdictions that do not or insufficiently apply the FATF Recommendations

1. Bank shall take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement. In addition to FATF Statements circulated by Reserve Bank of India from time to time, Bank shall also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. Bank shall also give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.
2. Bank shall examine the background and purpose of transactions with persons (Including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations. Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions shall, as far as possible be examined, and written findings together with all documents shall be retained and made available to Reserve Bank/other relevant authorities, on request.

7.0 REPORTING REQUIREMENTS

7.1 Reports to be furnished to FIU-IND

1 In terms of Rule 3 of the PML (Maintenance of Records) Rules, 2005, Bank is required to furnish information relating to cash transactions, cash transactions integrally connected to each other, and all transactions involving receipts by non-profit organizations (NPO means any entity or organization that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered (erstwhile Section 25 of Companies Act, 1956) under Section 8 of the Companies Act, 2013), cash transactions where forged or

counterfeit currency notes or bank notes have been used as genuine, cross border wire transfer, etc. to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address: The Director, FIU-IND, Financial Intelligence Unit-India, 6th Floor, Hotel Samrat, Chanakyapuri, New Delhi-110021. Website - http://fiuindia.gov.in/

2. FIU-IND has released a comprehensive reporting format guide to describe the specifications of prescribed reports to FIU-IND. FIU-IND has also developed a Report Generation Utility and Report Validation Utility to assist reporting entities in the preparation of prescribed reports. The Office Memorandum issued on Reporting Formats under Project FINnet dated 31st March, 2011 by FIU containing all relevant details are available on FIU's website.
3. In terms of Rule 8, while furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a misrepresented transaction beyond the time limit as specified in the Rule shall constitute a separate violation. Branches shall take note of the timeliness of the reporting requirements and submit the reports within the timelines. As a part of transaction monitoring mechanism, Bank shall put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of the customers. The software shall be robust enough to throw the alerts for effective identification and reporting of suspicious transactions.
4. As per Rule 7 of PML Rules, the procedure and manner of furnishing information shall be as under:
    i. The Bank shall communicate to the Director, FIU IND the name, designation and address of the Designated Director and the Principal Officer.
    ii. The Principal Officer shall furnish the information referred to sub-rule (1) of rule 3 to the Director on the basis of information available with the reporting entity. A copy of such information shall be retained by the Principal Officer for the purposes of official record
    iii. The Bank shall evolve an internal mechanism having regard to any guidelines issued by regulator, for detecting the transactions referred to in sub-rule (1) of rule 3 and for furnishing information about such transactions in such form as may be directed by its Regulator.
    iv. The Bank, its designated director, officers and employees shall observe the procedure and the manner of furnishing information as specified by its Regulator.

7.2 Cash Transaction Reports (CTR)

The bank shall scrupulously adhere to the following

1. The Cash Transaction Report (CTR) for each month shall be submitted to FIUIND by 15th of the succeeding month. Cash transaction reporting by branches to their controlling offices shall, therefore, invariably be submitted on monthly basis and Bank shall ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.
2. All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine shall be reported by the Principal Officer of the Bank to FIUIND in the specified format (Counterfeit Currency Report- CCR) by 15th day of the next month. These cash transactions shall also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.
3. While filing CTR, details of individual transactions below Rs.50000.00 need not be furnished

4. CTR shall contain only the transactions carried out by the Bank on behalf of their clients / customers excluding transactions between the internal accounts of the Bank.
5. A summary of cash transaction report for the Bank as a whole shall be compiled by the Principal Officer of the Bank every month in physical form as per the format specified. The summary shall be signed by the Principal Officer and submitted to FIU-IND. In case of Cash Transaction Reports (CTR) compiled centrally by banks for the branches having Core Banking Solution (CBS) at their central data centre level, banks may generate centralized Cash Transaction Reports (CTR) in respect of branches under Core Banking Solution at one point for onward transmission to FIU-IND, provided the CTR is generated in the format prescribed by FIU-IND.
6. A copy of the monthly CTR submitted to FIU-India in respect of the branches is available at the Bank for production to the auditors/ inspectors, when asked for
7. The instruction on 'Maintenance of records of transactions' and 'Preservation of records' as contained at Para 5 are scrupulously followed by the branches and other concerned.

7.4 Suspicious Transaction Reports (STR)

1. While determining suspicious transactions, Bank shall be guided by the definition of suspicious transaction as contained in PMLA Rules as amended from time to time
2. It is likely that in some cases transactions are abandoned/ aborted by customers on being asked to give some details or to provide documents. Bank shall report all such attempted transactions in STRs, even if not completed by the customers, irrespective of the amount of the transaction.
3. Bank shall make STRs if there is a reasonable ground to believe that the transaction involve proceeds of crime irrespective of the amount of transaction and / or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002
4. The Suspicious Transaction Report (STR) shall be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report shall be made available to the competent authorities on request.

5 In the context of creating KYC/ AML awareness among the staff and for generating alerts for suspicious transactions and for reporting, branches may consider the indicative list of suspicious activities as detailed below.

Rule Id	Rule Description	Event Type	Remarks
1	HIGH CASH CREDIT TRANSACTION 1000000 AND ABOVE	DAILY	CASH CREDIT 10 LAKH & ABOVE PER DAY IN SINGLE ACCOUNT
2	HIGH CASH CREDIT TRANSACTION 2000000 AND ABOVE	DAILY	CASH CREDIT 20 LAKH & ABOVE PER DAY IN SINGLE ACCOUNT
3	LARGE CASH WITHDRAWL AS COMPARED TO 25% OF	MONTHLY	CASH WITHDRAWL AS COMPARED TO 25 % OF TOTAL DEBIT IN ONE MONTH.

	TOTAL DEBIT		TOTAL DEBIT 1 LAKH AND ABOVE AND CASH WITHDRAWL 25 THOUSAND AND ABOVE IN 30 DAYS
4	LARGE CASH DEPOSIT AS COMPARED TO 50% OF TOTAL CREDIT	MONTHLY	CASH DEPOSIT AS COMPARED TO 50 % OF TOTAL CREDIT IN ONE MONTH. TOTAL DEPOSIT 1 LAKH AND ABOVE AND CASH DEPOSIT 50 THOUSAND AND ABOVE IN 30 DAYS
5	HIGH CREDIT TRANSACTION 1500000 AND ABOVE IN A MONTH	MONTHLY	HIGH CREDIT TRANSACTION 1500000 AND ABOVE IN A MONTH
7	TRANSACTIONS IN DORMAT/INOPERATIVE ACCOUNTS	DAILY	TRANSACTION IN ACCOUNT STATUS 4. INOPERATIVE / 5. DORMANT
8	HIGH CASH TRANSACTIONS IN NEW ACCOUNTS	MONTHLY	TRANSACTION IN ACCOUNT STATUS 2 . AMOUNT 2 LAKH & ABOVE IN 180 DAYS
9	RAPID MOVEMENT OF FUNDS.	WEEKLY	TOTAL CREDIT 10 LAKH AND ABOVE AND DEBIT 7.5 LAKH AND ABOVE IN 7 DAYS
10	DEBIT TRANSACTIONS JUST UNDER REPORTING THRESHOLD 450000 TO 500000	MONTHLY	SUM OF DEBIT TRANSACTIONS BETWEEN 4.5 LAKH TO 5 LAKH IN 30 DAYS
11	CREDIT TRANSACTIONS JUST UNDER REPORTING THRESHOLD 900000 TO 1000001	MONTHLY	SUM OF CREDIT TRANSACTIONS BETWEEN 9 LAKH TO 1000001 IN 30 DAYS
12	TRANSACTIONS IN STAFF ACCOUNTS ABOVE 100000 IN A MONTH	MONTHLY	TRANSACTION IN ACCOUNT TYPE 2 .AMOUNT 1 LAKH & ABOVE 30 DAYS
13	TRANSACTIONS IN TRUST ACCOUNTS ABOVE 100000 IN A MONTH	MONTHLY	TRANSACTION IN ACCOUNT TYPE 4 .AMOUNT 1 LAKH & ABOVE 30 DAYS

6. Bank shall not put any restrictions on operations in the accounts where an STR has been filed. Bank and their employees shall keep the fact of furnishing of STR strictly confidential, as required under PML rules. Moreover, it shall be ensured that there is no tipping off to the customer at any level.
7. **Recognizing and Reporting Suspicious Transaction/ Activity**

   The Rules notified under the PMLA Act, 2005 define a "Suspicious Transaction" as a transaction whether or not made in cash which to a person acting in good faith.
   i. Gives rise to a reasonable ground of suspicion that it may involve the proceeds of an offence specified in the schedule to the PML Act, 2005, regardless of the value involved
   ii. Appears to be made in circumstances of unusual or unjustified complexity ; or

   iii. Appears to have no economic rationale or bonafide purpose or

iv. Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

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

Suspicion is personal and subjective and falls far short of proof based on firm evidence. Suspicion may be defined as being beyond mere speculation and based on some foundation i.e., "A degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not"; and "Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation."

8. **Reasonable grounds to suspect'** introduces an objective test rather than the subjective test of suspicion. It might therefore be de defined in terms of 'wilful blindness' i.e., turning a blind eye to the obvious; or negligence i.e., willfully and recklessly failing to make the adequate enquiries that an honest person would be expected to make in the circumstances; or failing to assess adequately the facts and information that are either presented or available and that would put an honest person on enquiry. Branch staff may need to be able to demonstrate that they took all reasonable steps as a person acting in good faith would take in the particular circumstance; to know the customer and the rationale for the transaction or the instruction. Branches should submit STRs if they have reasonable ground to believe that the transaction involves proceeds of crime generally irrespective of the amount of transaction and/ or the threshold limit envisaged for predicate offences of PMLA, 2002.
9. In case of transactions carried out by a non-account based customer, that is walk – in customer, where the amount of transaction is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified. Further, if a branch has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000-00 the branch should verify the identity and address of the customer and also consider filing Suspicious Transaction Reports (STRs) immediately in appropriate cases, in the formats. In the reporting format specifications, the banks are required to provide information about the source of alert and the alert indicator(s) for detection of suspicious transactions.

7.5 Non-Profit Organization

The report of all transactions involving receipts by non-profit organizations of value more than Rs.10.00 Lakh or its equivalent in foreign currency should be submitted every month to the Director, FIU-IND by 15th of the succeeding month in the prescribed format.

8.0 GENERAL GUIDELINES

8.1 Confidentiality of customer information

The information collected from the customer for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling etc. Information sought from the customer shall be relevant to the perceived risk and be non-intrusive. Any other information that is
sought from the customer shall be called for separately only after the account has been opened, with his/her express consent and in a different form, distinctly separate from the application form. It shall be indicated clearly to the customer that providing such information is optional.

8.2 Secrecy Obligations and Sharing of Information

1. Bank shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer. While considering the requests for data/ information from Government and other agencies, Bank shall satisfy itself that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.
2. The exceptions to the said rule shall be as under

   i. Where there is a duty to the public to disclose

   ii. The interest of Bank requires disclosure and

   iii. Where the disclosure is made with the express or implied consent of the customer
3. **Avoiding hardship to customers**

   Branches should keep in mind the spirit of instructions issued by the RBI and avoid undue hardships to individuals who are otherwise classified as low risk customers
4. **Sensitising Customers**

   Implementation of AML/CFT policy may require certain information from customers of a personal nature or which had not been called for earlier. The purpose of collecting such information could be questioned by the customer and may often lead to avoidable complaints and litigation. Bank shall, therefore, prepare specific literature / pamphlets etc. to educate the customer regarding the objectives of the AML/CFT requirements for which their cooperation is solicited
5. **Hiring of Employees**

   KYC norms / AML standards / CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking channels. Therefore, Bank shall put in place adequate screening mechanism as an integral part of its personnel recruitment / hiring process.
6. **Employee Training**

   Bank shall have an ongoing employee training programme so that the members of the 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 needs to be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the bank, regulation and related issues shall be ensured.

7. **Technology requirements**

   The AML software in use at the Bank shall be comprehensive and robust enough to capture all cash and other transactions, including those relating to walk-in customers, third party products, and transactions involving internal accounts of the bank
8. **Designated Director**

   Bank has nominated the Chief Executive Officer of the Bank as a Designated Director of the Bank, as required under the provisions of the PML Rules, 2005, to ensure compliance with the obligations under the Act and Rules. The Designated

Director shall oversee the compliance position of AML norms in the Bank.

9. **Principal Officer**

i. Bank has appointed a Principal Officer. The Principal Officer shall be independent and report directly to the Senior Management/ Board of Directors.
ii. Principal Officer is responsible for monitoring KYC/AML compliance at operational units, escalation of suspicious transactions reported by branches through STRs and sharing of information as required under the law.
iii. He will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism.
iv. The role and responsibilities of the Principal Officer include overseeing and ensuring overall compliance with regulatory guidelines on KYC/ AML/ CFT issued from time to time and obligations under the Prevention of money Laundering Act, 2002, rules and regulations made there under, as amended from time to time.
v. The Principal Officer is responsible for timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by non-profit organizations of value more than Rs.10.00 Lakh or its equivalent in foreign currency to FIU-IND.
vi. The Principal Officer and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records and other relevant information.
vii. The Principal Officer under PMLA Act, 2002 shall be the competent authority for fixing the thresholds for generation of AML alerts and the periodicity of reviewing the alerts shall be at half yearly intervals or as and when required

10. **Need for photographs and address confirmation**

i. Pass port size/stamp size photograph of the depositors shall be obtained in case of all Current Accounts, SB accounts and Term Deposits.
ii. In case of joint accounts, partnership accounts, accounts of societies, clubs, associations, public/private limited companies, HUF, trusts, Limited Liability Partnerships etc., and those of minors, photographs of the authorized signatories should be obtained. Photographs of the student account holders should be attested by the school authorities on the reverse.
iii. In case of change in the authorized signatories, photographs of the new signatories are to be obtained duly countersigned by the competent authorities of the concerned institutions/ organizations.
iv. Where the accounts are operated by Letters of Authority, photographs of the authority holders should be obtained, duly attested by the depositors.

11. **Sale of third party products**

When Bank sells third party products as agent, the responsibility for ensuring compliance with KYC/ AML/ CFT regulations lies with the third party. However, to mitigate reputational risk to Bank and to enable a holistic view of a customer's transactions, branches are advised as follows:

i. Even while selling third party products as agents, branches should verify the identity and address of the walk-in customer.
ii. Branches should also maintain transaction details with regard to sale of third party products and related records for a period and in the manner prescribed in the relevant paragraph.
iii. Bank's AML software will capture, generate and analyze alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products

with customers including walk-in customers.

iv. Sale of third party products by branches as agents to customers, including walk-in customers, for Rs.50,000 and above must be

a. by debit to customer's account or against cheques and.

b. obtention & verification of the PAN given by the account based as well as walk-in customers

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

Sd/- Sd/-

Chief Executive Officer **President**