POLICY GUIDELINES

ON

KYC NORMS / AML STANDARDS / CFT MEASURES / OBLIGATION OF THE BANK UNDER PMLA, 2002.

Index

1. PURPOSE

RBI has advised Banks that a proper Policy on 'Know Your Customer [KYC]', 'Anti Money Laundering [AML]' and 'Combating of Financing of Terrorism [CFT]' measures and obligation of bank under Prevention of Money Laundering Act, 2002 be formulated and put in place.

The purpose of KYC/AML/CFT policy is to put in place customer identification procedures for opening of accounts and monitoring transactions in the accounts for detection of transactions of suspicious nature for the purpose of reporting to Financial Intelligence Unit-India [FIU-IND] in terms of the recommendations made by Financial Action Task Force (FATF) and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision (BCBS) on AML standards and on CFT measures.

For this Policy, the term 'Money Laundering' would also cover financial transactions where the end-use of funds is for financing terrorism, irrespective of the source of funds.

2. OBJECTIVE

The Policy has been framed to develop a strong mechanism for achieving the following objectives:

2.1 To prevent Bank from being used, intentionally or unintentionally, by criminal elements for Money Laundering or Terrorist Financing activities. KYC procedures also enable the Bank to know/understand their customers and their financial dealings better, which in turn helps them to manage the associated risks prudently.

2.2. To enable the Bank to comply with all the legal and regulatory obligations in respect of KYC / AML / CFT measures / Obligation of Bank under PMLA 2002 and to cooperate with various government bodies dealing with related issues.

3. DEFINITIONS

3.1 CUSTOMER

For the purpose of KYC Policy, a 'Customer' is defined as a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

3.2 Designated Director

"Designated Director" means a person designated by the reporting entity (bank, financial institution, etc.) to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and includes:-

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

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

3.3 "Officially valid document" (OVD)

OVD means the passport, the driving licence, the Permanent Account Number (PAN) Card, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number, or any other document as notified by the Central Government in consultation with the Regulator.

(i) Provided that where 'simplified measures' are applied for verifying the identity of the clients the following documents shall be deemed to be OVD:

a) identity card with applicant's Photograph issued by Central/ State Government Departments, Statutory/ Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
b) Letter issued by a gazetted officer, with a duly attested photograph of the person.

(ii) 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 :

a) Utility bill which is not more than **two** months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
b) Property or Municipal Tax receipt;
c) Bank account or Post Office savings bank account statement;
d) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
e) Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and
f) Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India.

3.4 Person

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

3.5 Transaction

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

` (i) opening of an account;

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

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

(iv) entering into any fiduciary relationship;

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

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

4 KYC POLICY

There are four pillars of KYC policy which are as under:

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

4.1. CUSTOMER ACCEPTANCE POLICY(CAP)

As a Customer Acceptance Policy, the Bank will verify the identity as laid down in Customer Identification Procedures and the Bank will:

i. not accept any person / entity barred by law of the land to avail banking facilities as its customer;

ii. not open accounts in the name of anonymous or fictitious/benami person(s) or account on behalf of other persons whose identity has not been disclosed or cannot be verified. Bank will also not receive remittance/conduct transactions

with regard to purchase/sale of foreign currency notes/ traveler cheques in respect of such persons;

iii. parameterize risk perception of the customer in terms of nature of business/activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status, etc. to enable categorization of customers into three types of risk categories viz., Low, Medium and High Risk, based on risk perception decided on acceptance criteria for each category of customers;

iv. ensure to obtain documents and other information in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money Laundering Act 2002 and instructions/guidelines issued by RBI from time to time.

v. not open an account where bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the Identity and/or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished to the bank. As regards KYC non-compliant accounts due to non-submission of KYC documents by customers, bank would impose 'partial freezing' on such KYC non-compliant accounts in a phased manner. While imposing 'partial freezing', bank 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, bank will 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' bank will disallow all debits and credits from / to the accounts, rendering them inoperative. During the course of such partial freezing, the account holders can revive their accounts by submitting the KYC documents as per instructions in force. In case the customer despite such measures, shows unwillingness to comply with KYC/AML/CFT requirements, bank is free to proceed further and close the accounts after issuing due notice to the customer in writing, explaining the reasons for such a decision. Such decision shall be taken by the Incumbent Incharge.

vi. not open accounts where identity of the customer matches with any person or entity, whose name appears in the sanction lists circulated by the Reserve Bank.

4.2. CUSTOMER IDENTIFICATION PROCEDURE(CIP).

4.2.1 General

(a) Customer Identification Procedure means:

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 OVDs, as per **Annexure-I.** Bank to obtain sufficient information to establish, to its satisfaction, the identity of each new customer, whether regular or occasion al, and the purpose of the intended nature of the banking relationship and be satisfied that due diligence has been observed based on the risk profile of the customer in compliance with

the extant guidelines in place. Such risk based approach is to avoid disproportionate cost to bank and a burdensome regime for the customers. Besides obtaining of valid proof of address, an independent verification of address will also to be carried out, by sending "Letter of Thanks" to the customer.

(b) The Customer Identification Procedure will be carried out at the time of:

(i) establishing banking relationship;
(ii) carrying out a financial transaction;
(iii) when the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data;
(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/-.
(vi) when carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected.
(vii) when the bank has a 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/-.

(c) Bank will seek mandatory information required for KYC purpose which the customer is obliged to give while opening an account or during periodic updation. Other optional customer details / additional information, if required, be obtained separately after the account is opened only with the explicit consent of the customer.

4.2.2 I. Customer Due Diligence requirements (CDD) while opening accounts.

A. Accounts of individuals:

(i) For opening accounts of individuals, Bank to obtain one certified copy of an 'officially valid document' containing details of identity and address, one recent photograph and such other documents pertaining to the nature of business and financial status of the customer as may be required.

(ii) E-KYC service of Unique Identification Authority of India (UIDAI) is also accepted as a valid process for KYC verification under the PML Rules. The information containing demographic details and photographs made available from UIDAI as a result of e-KYC process is treated as an 'Officially Valid Document'. Under e-KYC, the UIDAI transfers the data of the individual comprising name, age, gender, and photograph of the individual, electronically to the bank/business correspondents/business facilitators, which is accepted as valid process for KYC verification. The individual user, however, has to authorize to UIDAI by explicit consent to release her/his identity/address through biometric authentication to the banks/business correspondents/business facilitator. If the prospective customer knows only his/her Aadhaar number, the bank has to print the prospective customer's

e-Aadhaar letter in the bank directly from the UIDAI portal; or adopt e-KYC procedure as mentioned above. If the prospective customer carries a copy of the e-Aadhaar downloaded from a place/source elsewhere, still the bank has to print the prospective customer's e-Aadhaar letter in the bank directly from the UIDAI portal or adopt e-KYC procedure as mentioned above or confirm the identity and address of the resident through the authentication service of UIDAI.

(iii) Since introduction is not necessary for opening of accounts under PML Act and Rules or the Reserve Bank's extant instructions, Bank will not insist on introduction for opening of bank accounts. However, the due diligence at the time of accepting a customer is of utmost importance to avoid frauds. Spirit of KYC norms is to ensure the authenticity of OVD for identity and address of the customer. A certificate of having verified genuineness of Voter's ID Card / PAN Card must be appended on the photocopy of the documents and kept with AOF.

(iv) **Simplified Measures for Proof of Identity:**

If an individual customer does not have any of the OVDs as proof of identity, then Bank to adopt 'Simplified Measures' in respect 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 customers, where simplified measures are applied, it is sufficient to obtain a certified copy of any one of the documents referred to at proviso to paragraph 3.3 (i) above, which are deemed as an OVD for the purpose of proof of identity.

(v) **Simplified Measures for Proof of Address:**

The additional documents mentioned at 3.3(ii) above are deemed as 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.

(vi) **Small Accounts**

If an individual customer does not possess either any of the OVDs or the documents applicable in respect of simplified procedure (as detailed at paragraph 3.3 above), then 'Small Accounts' may be opened for such an individual. A 'Small Account' means a savings account in which:

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

Bank will allow to open a small account on the basis of self-attested photograph and affixation of signature or thumb impression as the case may be, on the Account Opening Form provided that:

(a) The Officer/ Manager/ Sr. Manager of a branch of the Bank [authorized as "Designated Officer" for the purpose of opening of small accounts], while opening the small account will certify under his signature that the person opening the account has affixed his signature or thumb impression, as the case may be, in his presence.

(b) It will be ensured that no foreign remittances are credited to a small account and that the stipulated limits on monthly and annual aggregate of transactions and balance in such accounts are not breached, before a transaction is allowed to take place;

© 'Small Accounts' shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months in case such account holder provides evidence to 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;

d) 'Small Accounts' shall be monitored and if there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of client shall be established through production of 'officially valid documents';

e) Foreign remittance shall not be allowed to be credited into small accounts unless the identity of the client is fully established through the production of officially valid documents.

(vii) A customer is required to submit only one 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.

(viii) 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 Bank to take a declaration from the customer of her/his local address on which all correspondence will be made by the Bank with the customer. No proof is required to be submitted by the customer for such address. This address, however, must be verified by the Bank through 'positive confirmation' such as acknowledgment of receipt of letter, cheque books, ATM cards; telephonic conversation; visits to the place; etc. In the event of any change in this address due to relocation or any other reason, customers will intimate the new address for correspondence to the Bank within two weeks of such a change.

(ix) In case the address mentioned as per 'proof of address' undergoes a change, fresh proof of address is to be submitted to the Bank within a period of six months.

(x) In case of close relatives, e.g. husband, wife, son, daughter and parents, 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, Bank to obtain 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 her/him. Bank to obtain OVD for proof of identity of the prospective customer. Bank will also obtain any other supplementary evidence such as letter received through post for further verification of the address of the proposed customer.

(xi) Bank will not insist to obtain fresh documents of the customer when the customer approaches it for transferring his/her account from one branch to another branch. Bank will ensure that KYC verification once done by the transferor branch will be valid for the transferee branch if full KYC verification has been done for the concerned account and is not due for periodic updation. The customer will be allowed to transfer his account from one branch to another branch without restrictions, without insisting on fresh proof of address and/or identity and on the basis of a self-declaration from the account holder about his/her current address. Further, if an existing KYC compliant customer desires to open another account in the bank, there is no need for submission of fresh proof of identity and/or address.

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

(xiii) For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Bank will rely on a third party subject to the conditions that:-

(1) the Bank immediately obtains necessary information of such client due diligence carried out by the third party;

(2) the Bank 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;

(3) the Bank 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;

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

(5) the Bank is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.

(xiv) Accounts of Non- face- face customers

In case of non-face-to-face customers, in addition to the usual customer identification procedures, enhanced due diligence will be ensured. The prospective customers will be required to submit certified copies of all the documents presented for the purpose of identification to the satisfaction of the Bank. [If necessary, additional documents may be called for]. As an additional precaution, in such cases, the first payment is to be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards.

In the case of cross-border customers, the Bank will ensure that the third party certifying the supporting documents is regulated and supervised entity and has adequate KYC systems in place.

(xv) **Procedure to be followed in respect of foreignstudents.**

Banks will follow the following procedure for foreign students studying in India:

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

(2) Bank will obtain a declaration about the local address within a period of 30 days of opening the account and verify the said local address.

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

(4) The account will be treated as a normal NRO account, and will be operated in terms of instructions contained in the Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of Schedule 3 of FEMA Notification 5/2000 RB dated May 3, 2000.

(5) Students with Pakistani and Bangladesh nationality will need prior approval of the Reserve Bank for opening the account.

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

(a) Politically Exposed Persons (PEPs) are individuals who are or have been entrusted with prominent public positions/functions in a foreign country, e.g., Heads of States or of Governments, Senior politicians, Senior Government/Judicial/Military officers, Senior Executives of state-owned corporations, important political party officials etc. Bank will ensure enhanced due diligence and will gather sufficient information on any person/customer of the category of PEPs intending to establish a banking relationship and try to collect and check all information available on the person in the public domain. Bank will also verify the identity of the person and seek information about the sources of funds before accepting

PEP as customer. Such accounts will be subjected to enhanced monitoring on an ongoing basis.

(b) Decision to open an account including existing customers or the beneficial owner of an existing account subsequently becoming a PEP will be taken at Senior Management Level i.e at the level of Chief Manager and above.

© In the event of existing customers or the beneficial owner of an existing account subsequently becoming a PEP, the approval of the Chief Manager and above will be obtained to continue the business relationship and subject the account to the enhanced due diligence measures as applicable to the customers of PEP category including enhanced monitoring on an on-going basis. The said norms will also apply to the accounts of the family members or close relatives of PEPs. Such type of Customers requiring very high level of monitoring will be categorized as 'High Risk'. These instructions are also applicable to accounts where PEP is the ultimate beneficial owner.

B. Accounts of persons other than individuals:

` **(i) Where the customer is a company**, one certified copy each of the following documents are required for customer identification:

(a) Certificate of incorporation;
(b) Memorandum and Articles of Association;
(c) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf and
(d) An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf.

Bank to remain vigilant against business entities being used by individuals as a 'front' for maintaining accounts with bank. Bank to 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 are to be moderated according to the risk perception e.g. in the case of a public company it is not necessary to identify all the shareholders.

(ii) Where the customer is a partnership firm, one certified copy of the following documents is required for customer identification:

(a) registration certificate;
(b) partnership deed and
(c) an officially valid document in respect of the person holding an attorney to transact on its behalf.

(iii) Where the customer is a trust, one certified copy of the following documents is required for customer identification:

(a) registration certificate;

(b) trust deed and
(c) an officially valid document in respect of the person holding a power of attorney to transact on its behalf.

(iv) Where the customer is an unincorporated association or a body of individuals, one certified copy of the following documents is required for customer identification:

(a) resolution of the managing body of such association or body of individuals;
(b) power of attorney granted to transact on its behalf;
(c) an officially valid document in respect of the person holding an attorney to transact on its behalf and
(d) such information as is required by the bank to collectively establish the legal existence of such an association or body of individuals.

(v) Proprietary concerns*:*

(1) For proprietary concern, 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:

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

(2) However, in case where the Bank is satisfied that it is not possible to furnish two such documents in the name of proprietary concern , the Bank may accept only **one** of the above mentioned documents as activity proof provided that the Bank undertakes contact point verification, collects such information as is required to establish the existence of such firm, confirms, clarifies and satisfies itself that the business activity is verified from the address of the proprietary concern**.**

These guidelines on proprietorship concerns will apply to all new customers and to all existing customers also.

(vi) Simplified KYC norms for Foreign Portfolio Investors (FPIs).

In terms of Rule 9 (14)(i) of the PML Rules, simplified norms have been prescribed for those FPIs who have been duly registered in accordance with

SEBI guidelines and have undergone the required KYC due diligence / verification prescribed by SEBI through a Custodian / Intermediary regulated by SEBI. Such eligible / registered FPIs may approach a bank for opening a bank account for the purpose of investment under Portfolio Investment Scheme (PIS) for which KYC documents as detailed in Annex II of KYC-AML circular No. 25/2014 dated 20.06.2014 will be required. Category I FPIs are, however, not required to submit the undertaking that "upon demand by Regulators / Law Enforcement Agencies the relative documents / s will be submitted to the bank." For this purpose, bank will rely on the KYC verification done by the third party (i.e. the Custodian/SEBI Regulated Intermediary) subject to the conditions laid down in Rule 9 (2) [(a) to (e)] of the PML Rules.

(vii) <u>Pooled Accounts-Accounts opened by professional intermediaries:</u>

When the Bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified by applying KYC norms. Bank may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Bank, however, will not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the bank. Where funds held by the intermediaries are not co-mingled at the bank and there are 'sub- accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the bank, the bank should still look into the beneficial owners. Where the bank relies on the 'customer due diligence' (CDD) done by an intermediary, the bank must 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. The ultimate responsibility for knowing the customer lies with the bank.

A gist of documents that can be accepted as proof of identity and address for various categories is furnished in Annex I.

C. Beneficial Ownership

When the Bank identifies a customer for opening an account, it will identify the beneficial owner(s) and take all reasonable steps in terms of Rule 9(3) of the PML Rules to verify his identity, as per guidelines provided below:

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

Explanation- For the purpose of this sub-clause-

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

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

(b)Where the **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/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.

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

(d)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.

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

(f) Where the **client or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a com**pany, 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 will determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, bank will 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 should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

II. INTRODUCTION OF NEW TECHNOLOGY PRODUCTS – INTERNET BANKING / CREDIT CARDS / DEBIT CARDS / SMART CARDS / GIFT CARDS

a) Bank will pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking. The Bank will not provide internet facility/technology product to any person without compliance of KYC guidelines and without customer's specific request/understanding of the product. Bank will ensure that full KYC/AML procedures are duly applied before providing internet facility / issuing credit cards / debit cards / smart cards / gift cards etc. including on the add-on/supplementary cardholders.

b) The amount transferred / received through electronic mode, beyond a threshold limit, of Rs. 50,000/- and above would be to the debit of the accounts of the customers concerned.

c) The agent, if any, engaged or appointed for the purpose of marketing of any product including credit cards / debit cards / smart cards / gift cards etc., would also be subjected to due diligence and full KYC measure.

III. Periodic Updation of KYC.

A. CDD requirements for periodic updation:

Bank to carry out periodical updation of KYC information of every customer, which includes the following:

(i) KYC exercise be done at least every two years for high risk customers, every eight years for medium risk customers and every ten years for low risk customers. Such KYC exercise will include all measures for confirming the identity and address and other particulars of the customer that the Bank considers reasonable and necessary based on the risk profile of the customer, taking into account whether and when client due diligence measures were last undertaken and the adequacy of data obtained.

(ii) Bank not to seek fresh proofs of identity and address at the time of periodic updation, from those customers who are categorized as 'low risk', in case there is no change in status with respect to their identities and addresses. A self-certification by the customer to that effect will 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. Bank will not insist on physical presence of such low risk customer at the time of periodic updation. The time limits prescribed at (i) above will apply from the date of opening of the account/ last verification of KYC.

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

B. Freezing and closure of accounts.

(i) In case of non-compliance of KYC requirements by the customers despite repeated reminders by bank, Bank will impose 'partial freezing' on such KYC non-compliant accounts in a phased manner.

(ii) During the course of such partial freezing, the account holders can revive their accounts by submitting the KYC documents as per instructions in force.

(iii) While imposing 'partial freezing', Bank 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 to be followed by a reminder giving a further period of three months.

(iv) Thereafter, Bank will impose 'partial freezing' by allowing all credits and disallowing all debits with the freedom to close the accounts.

(v) If the accounts are still KYC non-compliant after six months of imposing initial 'partial freezing' Bank will disallow all debits and credits from/to the accounts thereby, rendering them inoperative.

(vi) Further, it will always be open to the Bank to close the account of such customers after issuing due notice to the customer explaining the reasons for taking such a decision. Such decision shall be taken by the Incumbent Incharge.

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

IV. Miscellaneous.

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

In case the bank has arrangements with co -operative banks wherein the latter open current accounts with the bank and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in- customers for effecting their remittances and payments. Since the 'at par' cheque facility offered by bank to co-operative banks is in the nature of correspondent banking arrangement, bank will monitor and review such arrangements to assess the risk including credit risk and reputational risk arising there from. For this purpose, bank will retain the right to verify the records maintained by the client cooperative banks/ societies for compliance with the extant instructions on KYC and AML under such arrangements.

In this regard, Urban Cooperative Banks (UCBs) are to utilize the 'at par' cheque facility only for the following purposes:

(i) For their own use.

(ii) For their account holders who are KYC complaint provided that all transactions of Rs.50,000/- or more should be strictly by debit to the customer's account.

(iii) For walk-in customers against cash for less than Rs.50,000/- per individual.

In order to utilise the 'at par' cheque facility in the above manner, UCBs to maintain the following:

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

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

UCBs to also ensure that all 'at par' cheques issued by them are crossed 'account payee' irrespective of the amount involved

B. Operation of Bank Accounts & Money Mules.

"Money Mules" are used to launder the proceeds of fraud schemes (*e.g.,* phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "money mules". In order to minimize the operations of such mule accounts, Bank to strictly adhere to the guidelines on opening of accounts and monitoring of transactions.

C. Simplified norms for Self Help Groups (SHGs)

KYC verification of all the members of SHG need not be done while opening the savings bank account of the SHG 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.

D. Walk-in Customers

Customer identification procedure will also be carried out in respect of walk-in-customers (non-account based customer) approaching Bank for transactions equal or exceeding Rs.50,000/- [Rupees fifty thousand] , whether conducted as a single transaction or series of transactions that appear to be connected. However, in case Bank has reason to believe that customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000/-, Bank will verify identity and address of customer and in case of suspicion may consider filing of Suspicious Transaction Report (STR) to FIU-India.

Note: In terms of Prevention of Money Laundering Rules, 2005, Banks are required to verify identity of customers of all international money transfer operations.

E. Issue of Demand Drafts, etc, for more than Rs.50,000/-

Bank will ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travellers' cheques for value of Rs.50,000/- and above is effected by debit to the customer's account or against cheques and not against cash payment.

Bank will 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.

F. Unique Customer Identification Code [UCIC].

A Unique Customer Identification Code (UCIC) will help Bank to identify the customers, avoid multiple identities, track the facilities availed, monitor financial transactions in a holistic manner and enable Bank to have a better approach to risk profiling of customers. Bank to allot UCIC while entering into new relationships with individual customers as also the existing customers.

4.3 Monitoring of Transactions.

4.3.1 Ongoing monitoring.

Ongoing monitoring is an essential element of effective KYC/AML procedures. Bank will 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 is based on the following principles:

(a) The extent of monitoring depends on the risk category of the account. High risk accounts have to be subjected to more intensified monitoring.

(b) Bank to 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.

© Bank has already customized software [finDNA] for the purpose of monitoring AML alerts based on the pre-defined scenarios. These scenarios will be periodically reviewed to make these more effective based on the feedback received and experience gained.

(d) Bank will periodically review the risk categorization of those accounts which require the need for applying enhanced due diligence measure. Such review of risk categorisation of customers should be carried out at a periodicity of not less than once in **six** months.

(e) Bank to closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies. In the accounts where large number of cheque books have been sought by the company and 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, the operations in such accounts will be analyzed and in case any unusual operations or suspicious transactions are noticed in the accounts, the matter will be immediately reported to Reserve Bank and other appropriate authorities such as FIU-IND.

4.4 Risk Management

Bank will 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 its knowledge about the clients, their business and risk profile and where necessary, the source of funds.

4.4.1 Internal control system

(i) A Senior Officer in the rank of Chief Manager or AGM working at the Circle Office (preferably looking after Inspection) will be nominated as Compliance-cum-Dy. Money Laundering Reporting Officer (DMLRO), who would be responsible for compliance of KYC / AML guidelines.

(iii) Incumbent Incharge of branches will allocate duties and responsibilities for opening of accounts through an Office Order to the staff members. Senior Officers from the Regional Offices, during their visits to the branches will ensure that monitoring of KYC / AML measures are being strictly adhered to as per the laid down procedures, keeping in view the risk involved in a transaction, account or banking/business relationship.

(iii) At the end of every calendar quarter, implementation and compliance of concurrent audit reports on adherence to KYC-AML guidelines at branches would be reviewed for apprising Audit Committee of Board.

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

(b) Bank to categorize its customers into low, medium and high risk category based on its 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 nature and extent of due diligence, may 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, is 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. Further, Non-Profit Organisations (NPOs)/ Non-Government Organisations (NGOs) promoted by the United Nations or its agencies, and such international/ multilateral organizations of repute, is also classified as low risk customers.

(ii) Customers who are likely to pose a higher than average risk are 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, accounts of bullion dealers (including sub-dealers), jewelers

and Politically Exposed Persons (PEPs) of foreign origin etc. are categorized as high risk.

(iii) Other customers to be categorized as high risk are:

a. Non-resident customers;
b. High net worth individuals;
c. Trusts, charities; NGOs and organizations receiving donations;
d. Companies having close family shareholding or
e. Beneficial ownership; firms with 'sleeping partners';
f. Politically Exposed Persons [PEPs] of foreign origin; customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner,
g. Non-face to face customers and
h. Those with dubious reputation as per public information available etc.

(iv) In addition to what has been indicated above, take steps to identify and assess the ML/TF risk for customers, countries and geographical areas as also for products / services / transactions / delivery channels and will frame policies, controls and procedures with the approval of the boards, to effectively manage and mitigate the risk adopting a risk-based approach as per the initiative taken by IBA. Bank will adopt enhanced measures as per the indicative list of various types of indicators i.e. customer behavior and risk based transaction monitoring; High & Medium Risk: customers/ Products & Services/Geographies/ Locations/ Alerts for branches/ departments that should trigger suspicion at the time of processing of customer's transaction and not in line with customer's profile as given in Annexure-II.

5. Correspondent Banking and Shell Bank

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

(a) Gather sufficient information to fully understand the nature of business of the bank including information on management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the bank's home country.
(b) The accounts of the correspondence banks will be opened with the prior approval of International Banking Division, Head Office, who would also be doing the due diligence in terms of the guidelines issued by RBI and Govt. of India.
(c) The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented.
(d) In case of payable-through-accounts, the correspondent bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them.
(e) The correspondent bank should ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

(f) Bank should be cautious while continuing relationships with correspondent banks located in jurisdictions which have strategic deficiencies or have not made sufficient progress in implementation of FATF Recommendations.
(g) Bank to ensure that its respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.
(h) Bank will not enter into a correspondent relationship with a **"**shell bank**"** (i.e., a bank which is incorporated in a country where it has no physical presence and is not affiliated to any regulated financial group).
(i) The correspondent bank will not permit its accounts to be used by shell bank.

6. WireTransfer

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

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

(i) 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 could be the same person.
(ii) 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.
(iii) 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.
(iv) 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.

(b) Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analysing suspicious or unusual activity and disseminating the same. 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 to ensure that all wire transfers are accompanied by the following information:

1. Cross-border wire transfers

(i) All cross-border wire transfers must be accompanied by accurate and meaningful originator information.

(ii) Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included.

(iii) Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (ii) above.

2. Domestic wire transfers

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

(ii) If a bank has reason to believe that a customer is intentionally structuring wire transfer to below Rs.50,000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the bank must insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be made to FIU-IND.

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

(c) Exemptions

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

(d) Role of Ordering, Intermediary and Beneficiary banks

(i) Ordering Bank

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

(ii) Intermediary bank

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

2002) by the receiving intermediary bank of all the information received from the ordering bank.

(iii) Beneficiary bank

A beneficiary bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they should be reported to the Financial Intelligence Unit -India. The beneficiary bank should also take up the matter with the ordering bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information on the remitter, the beneficiary bank should consider restricting or even terminating its business relationship with the ordering bank.

7. Maintenance of KYC documents and Preservation period.

PML Act and Rules cast certain obligations on the bank in regard to maintenance, preservation and reporting of customer account information. Hence, Bank to ensure compliance with the requirements of PML Act and the Rules.

7.1 Maintenance of records of transactions.

Bank to maintain proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005), as mentioned below:

(i) All cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;

(ii) Series of all cash transactions individually valued below Rupees Ten Lakh, or its equivalent in foreign currency which are that have taken place within a month and the monthly aggregate which exceeds rupees ten lakhs or its equivalent in foreign currency. For the purpose of determining 'integrally connected transactions' 'all accounts of the same customer' is taken into account. However, individual entries below Rs. 50,000/- need not be reported in the Cash Transaction Report.

(iii) All transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency.

(iv) 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

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

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

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

7.2 Preservation of Records.

Bank 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.

(i) In terms of PML Amendment Act 2012, Bank will maintain for at least five years from the date of transaction between the bank and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

(ii) Bank to preserve the records pertaining to the identification of the customers and their address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills, etc.) obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended as required under Rule 10 of the Rules. The identification of records and transaction data should be made available to the competent authorities upon request.

(iii) Bank to maintain records of the identity of their clients, and records in respect of transactions referred to in Rule 3 in hard or soft format.

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

8. Combating Financing Terrorism.

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). The Bank will ensure before opening the account that the name(s) of the

proposed customer does not appear in the lists of designated/banned individuals/entities circulated by RBI/Bank from time to time.

(a) **The "Al-Qaida Sanctions List",** includes names of individuals and entities associated with the Al-Qaida. The Updated Al-Qaida Sanctions List is available at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml.

(b) The **"1988 Sanctions List",** consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at http://www.un.org/sc/committees/ 1988/list.shtml.

The United Nations Security Council Resolutions (UNSCRs), received from Government of India, are circulated by the Reserve Bank to all banks and Bank to update the lists and take them into account for implementation of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967.

Bank will also scan all the existing accounts to ensure that no account is linked to any of the individuals/entities in the list. In case the full details of accounts bearing resemblance with ant of the individuals/entities in the list, the branch will report to KYC-AML Cell, Head Office for submitting report to FIU-IND.

8.1 Freezing of Assets underSection51A ofUnlawfulActivities (Prevention)Act, 1967.

(a) The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. 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.

(b) Bank to strictly follow the procedure laid down in the UAPA Order dated August 27, 2009 (Annex II) and ensure meticulous compliance to the Order issued by the Government.

8.2 Jurisdictions that do not or insufficiently apply the Financial Action Task Force(FATF) Recommendations.

(a) Bank will take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement circulated from time to time. Bank will also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. Further, Bank will 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.

(b) Bank will examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions

included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations. Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible be examined, and written findings together with all documents should be retained and made available to Reserve Bank/other relevant authorities, on request.

9. Reporting Requirements.

(a) **Reporting to Financial Intelligence Unit - India**

(i) In terms of the 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 organisations (NPO means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered (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).

(ii) In terms of Rule 8, while furnishing information to the Director, FOI-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall constitute a separate violation. Bank to take note of the timelines of the reporting requirements.

(c) Reports to be furnished to Financial Intelligence Unit – India.

1. Cash Transaction Report (CTR).

(i) Report of all cash transactions of the value of more than rupee ten lakhs or its equivalent in foreign currency and all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transaction exceeds Rupees ten lakh. However, individual entries below Rs. 50,000/- will not be reported in the Cash Transaction Report.

(ii) The CTR for each month will be submitted to FIU-IND by 15th of the succeeding month.

(iii) A copy of monthly CTR submitted on its behalf to FIU-IND is available at the concerned branch (through MIS Report: Misc Reports Module under SENSRPT – 5/7 & 5/7a) for production to auditors/Inspectors, when asked for.

2. Suspicious Transaction Reports (STR).

(i) While determining suspicious transactions, bank will be guided by the definition of suspicious transaction as contained in PMLA Rules as amended from time to time.

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

(iii) Bank to submit STRs if it has reasonable ground to believe that the transaction involves proceeds of crime irrespective of the amount of the transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

(iv) Bank will ensure furnishing of STR within seven days of arriving at a conclusion by the Principal Officer of the Bank that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.

(v) Bank will ensure not to put any restrictions on operations in the accounts where an STR has been filed. The submission of STR will be kept strictly confidential, as required under PML Rules and it will be ensured that there is no tipping off to the customer at any level.

(vi) The primary responsibility for monitoring and reporting of suspicious transaction shall be of the branch. The monitoring of the transactions will also be done by controlling offices, who will also interact with the branches to facilitate monitoring and reporting of suspicious transactions.

3. Counterfeit Currency Report (CCR)

Cash transactions were forged or counterfeit currency notes have been used as genuine or where any forgery of a valuable security or document has taken place facilitating the transactions will be reported to Financial Intelligence Unit-India in the specified format not later than seven working days from the occurrence of such transactions.

4. Non Profit OrganisationsTransaction report [NTR]

Bank will report all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency to the Director, Financial Intelligence Unit-India by the 15th of the succeeding month.

5 Cross-border WireTransfer [CWTR]

Bank will file Cross-Border Wire Transfer Report (CWTR) to the Director, Financial Intelligence Unit-India by 15th of succeeding month for all cross

border wire transfers of the value of more than Rs 5 lakh or its equivalent in foreign currency where either the origin or destination of fund is in India.

10. General Guidelines.

(i) Confidentiality of customer information:

Information collected from customers for the purpose of opening of account be treated as confidential and details thereof not to be divulged for the purpose of cross selling, etc. Information sought from the customer be relevant to the perceived risk and be non-intrusive. Any other information, sought from the customer, 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, indicating clearly to the customer that providing such information is optional.

(ii) Avoiding hardship to customers:

While issuing operational instructions to branches, bank will keep in mind the spirit of the instructions issued by the Reserve Bank so as to avoid undue hardships to individuals who are otherwise classified as low risk customers.

(iii) 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 to prepare specific literature/pamphlets, etc., to educate the customer regarding the objectives of the AML/CFT requirements for which their cooperation is solicited.

(iv) Hiring of Employees

In order to ensure that the criminals do not misuse the banking channels, it would be ensured that adequate screening mechanism is put in place so that the right type of persons are recruited / hired.

(v) Employee training:

Bank will ensure to have an ongoing employee training programme so that the members of staff are adequately trained in AML/CFT policy. The focus of the training should 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 will be ensured.

(vi) Provisions of Foreign Contribution (Regulation) Act (FCRA).

Bank will ensure that the provisions of the Foreign Contribution (Regulation) Act, 2010, wherever applicable, are strictly adhered to.

(vii) **Applicability to overseas branches/subsidiaries.**

The guidelines in this circular apply to the branches and majority owned subsidiaries located abroad, to the extent local laws in the host country permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of the Reserve Bank. In case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of banks are required to adopt the more stringent regulation of the two.

(viii) **Technology requirements:**

The AML software in use at bank needs to be comprehensive and robust enough to capture all cash and other transactions, including those relating to walk-in customers, sale of gold/silver/platinum, payment of dues of credit cards/reloading of prepaid/travel cards, third party products, and transactions involving internal accounts of the bank.

(ix) **Designated Director***:*

Bank to nominate a Director on the Board as "designated Director", as per provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Rules), to ensure compliance with the obligations under the Act and Rules. The name, designation and address of the Designated Director be communicated to the FIU-IND. However, in no case, the Principal Officer should be nominated as the 'Designated Director'.

(x) **Principal Officer:**

(i) Bank to appoint a senior officer in the rank of General Manager as Principal Officer, who will supervise and monitor all the activities in respect of KYC/AML/CFT measures. The Principal Officer will act independently and report directly to the MD & CEO / ED.

(ii) Principal Officer 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. Principal Officer will be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law / regulations. The name, designation and address of the Principal Officer be communicated to the FIU-IND.

(iii) The Principal Officer will also be responsible for timely submission of CTRs/STRs/CCRs/NTRs/CBWTRs to FIU-India.

(iv) For effective monitoring of the transactions and smooth implementation of advanced tool of Anti-Money Laundering at bank level, an officer of the rank of Asstt. General Manager / Chief Manager will be designated as Money Laundering Reporting Officer (MLRO), who will report to Principal Officer of the bank.

(v) At Circle Offices, a Chief Manager or AGM (preferably looking after Inspection) will be designated as Compliance-cum-Dy. Money Laundering Reporting Officer (DMLRO), who will be responsible for compliance of KYC / AML guidelines in the Circle.

(vi) For discharging the responsibilities effectively, the Principal Officer and other appropriate staff should have timely access to Customer Identification Data and other Customer Due Diligence information, transaction records and other relevant information.

ANNEXURE-1

Customer Identification Procedure

Documents to be obtained from customers.

Types of Customers	Description of Documents Certified copy of any **one** of the following officially valid document [Copy verified from the original will be kept on record with AOF].
Accounts of Individuals Proof of Identity and Address	1. Passport 2. Permanent Account Number (PAN) Card 3. Voter's Identity Card issued by the Election Commission of India 4. Driving license 5. Job card issued by NREGA duly signed by an officer of the State Government. 6. The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number. Where 'simplified measures' are applied for verifying the identity of customers (low risk categorized customers) the following documents shall be deemed to be 'officially valid documents: (i) Identity Card with applicant's photograph issued by Central / State Government. Departments, Statutary / Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions. (ii) Letter issued by a gazetted officer, with a duly attested photograph of the person. Where 'simplified measures' are applied for verifying for the limited purpose of proof of address the following additional documents are deemed to be 'officially valid documents' (OVDs) : (i) Utility bill which is not more than two months old of any service provider (electricity, telephone, postpaid mobile phone, piped gas, water bill); (ii) Property or Municipal Tax receipt; (iii) Bank account or Post Office savings bank account statement; (iv) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; (v) Letter of allotment of accommodation from employer

	issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and (vi) Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India. ***Note:*** *A customer is required to submit only one OVD for both proof of identity and for proof of address as part of KYC procedure. If the OVD 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.*
Accounts of Companies	**In addition to KYC documents of the Directors of the company, the following documents should be obtained:** ▪ Certificate of Incorporation ▪ Certificate of Commencement of Business (in case of Public Ltd Co.) ▪ Memorandum & Articles of Association duly certified by a Director/Secretary as true copy. ▪ A copy of the latest Audited Balance Sheet & Profit and Loss Account in case of Public Ltd. Company. ▪ A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on behalf. and ▪ An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf.
Accounts of Partnership firms	**In addition to KYC documents of all partners/authorized persons of the concern, the following documents be obtained:** ▪ Registration Certificate. ▪ Partnership Deed. ▪ An officially valid document in respect of the person holding an attorney to transact on its behalf.
Accounts of Proprietorship concerns - Proof of the name, address and activity of the concern	**In addition to KYC documents of the Proprietor, any <u>two</u> of the following documents in the name of the proprietary firm:** ▪ Registration Certificate (in the case of registered concern); ▪ Certificate/licence issued by the Municipal authorities under Shop & Establishment Act; ▪ Sales and Income Tax Returns ▪ CST/VAT Certificate ▪ Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities ▪ Licence / certificate of practice issued in the name of proprietary concern by any professional body incorporated under statue. The complete income tax

	the sole proprietor where the firm's income is reflected, duly authenticated / acknowledged by the Incoe Tax Authorities. ***Note:*** *However, in cases where the Bank is satisfied that it is not possible to furnish two such documents in the name of proprietary concern , the Bank may accept only one of the above mentioned documents as activity proof provided that the Bank undertakes contact point verification, collects such information as is required to establish the existence of such firm, confirms, clarifies and satisfies itself that the business activity is verified from the address of the proprietary concern.*
Accounts of trusts	**In addition to KYC documents of the Managing Trustees/Founders/Managers/ Directors and their addresses, the following documents of Trust are to be obtained:** ▪ Registration certificate ▪ Trust Deed ▪ An officially valid document in respect of the person holding a power of attorney to transact on its behalf.
Accounts of unincorporated association or a body of individuals	**In addition to KYC documents of the Founders/Managers/ Directors and their addresses, the following documents of Trust are to be obtained:** ▪ Resolution of the managing body of such associations or body of individuals. ▪ Power of attorney granted to him to transact on its behalf. ▪ An officially valid document in respect of the person holding an attorney to transact on its behalf. ▪ Copy of Bye Laws
Accounts of Hindu Undivided Family	**In addition to KYC documents of Karta and Major Co-parceners, the following documents should be obtained**: ▪ Declaration of HUF and its Karta ▪ Recent Passport Photographs duly self attested by Karta and major co-parceners. ▪ Names and addresses of Karta and Major Co-parceners. ▪ An officially valid document in respect of the person holding an attorney to transact on its behalf.

ANNEXURE–II

INDICATIVE LIST OF VARIOUS TYPES OF INDICATORS I.E.CUSTOMER BEHAVIOUR AND RISK BASED TRANSACTION MONITORING, HIGH & MEDIUM RISK: CUSTOMERS/ PRODUCTS & SERVICES/ GEOGRAPHIES/ LOCATIONS/ALERTS FOR BRANCHES/ DEPARTMENTS

1. INDICATIVE LIST OF CUSTOMER BEHAVIOUR & RISK BASED TRANSACTION MONITORING

i. Customers who are reluctant in providing normal information while opening an account, providing minimal or fictitious information or when applying to open an account, providing information that is difficult or expensive for the institution to verify.
ii. Customer expressing unusual curiosity about secrecy of information involved in the transaction.
iii. Customers who decline to provide information that in normal circumstances would make the customer eligible for banking services.
iv. Customer giving confusing details about a transaction.
v. Customer reluctant or refuses to state a purpose of a particular large / complex transaction/ source of funds involved or provides a questionable purpose and / or source.
vi. Customers who use separate tellers to conduct cash transaction or foreign exchange transactions.
vii. Customers who deposit cash / withdrawals by means of numerous deposit slips / cheques leaves so that the total of each deposits is unremarkable, but the total of all credits / debits is significant.
viii. Customer's representatives avoiding contact with the branch.
ix. Customers who repay the problem loans unexpectedly.
x. Customers who appear to have accounts with several institutions within the same locality without any apparent logical reason.
xi. Customers seeks to change or cancel a transaction after the customer is informed of currency transaction reporting / information verification or record keeping requirements relevant to the transaction.
xii. Customer regularly issues large value cheques without balance and then deposits cash.
xiii. Sudden transfer of funds from unrelated accounts through internet (or such other electronic channels) and subsequent quick withdrawal through ATM.

A. Transactions Involving LargeAmounts of Cash

i. Exchanging an unusually large amount of small denomination notes for those of higher denomination;
ii. Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;
iii. Frequent withdrawal of large amounts by means of cheques, including traveller's cheques;
iv. Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;
v. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;
vi. Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits

normally associated with the normal commercial operations of the company, e.g. cheques, letters of credit, bills of exchange etc.;

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

B. Transactions that donot make EconomicSense

i. A customer having a large number of accounts with the same bank, with frequent transfers between different accounts;

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

C. Activitiesnot consistent with\theCustomer'sBusiness

i. Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.
ii. Corporate accounts where deposits & withdrawals by cheque/telegraphic transfers/foreign inward remittances/any other means are received from/made to sources apparently unconnected with the corporate business activity/dealings.
iii. Unusual applications for DD/TT/PO against cash.
iv. Accounts with large volume of credits through DD/TT/PO whereas the nature of business does not justify such credits.
v. Retail deposit of many cheques but rare withdrawals for daily operations.

D. Attempts to avoid Reporting/Record-keeping Requirements

i. A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
ii. Any individual or group that coerces/induces or attempts to coerce/induce a bank employee not to file any reports or any other forms.
iii. An account where there are several cash deposits/withdrawals below a specified threshold level to a avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

E. Unusual Activities

i. An account of a customer who does not reside/have office near the branch even though there are bank branches near his residence/office.
ii. A customer who often visits the safe deposit area immediately before making cash deposits, especially deposits just under the threshold level.
iii. Funds coming from the list of countries/centers, which are known for money laundering.

i. A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors, or its locations.
ii. A customer/company who is reluctant to reveal details about its activities or to provide financial statements.
iii. A customer who has no record of past or present employment but makes frequent large transactions.

G. Certain Suspicious Funds Transfer Activities

i. Sending or receiving frequent or large volumes of remittances to/from countries outside India.
ii. Receiving large TT/DD remittances from various centers and remitting the consolidated amount to a different account/center on the same day leaving minimum balance in the account.
iii. Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire/funds transfer.

H. Certain Bank Employees arousing Suspicion

i. An employee whose lavish lifestyle cannot be supported by his or her salary.
ii. Negligence of employees/willful blindness is reported repeatedly.

I. Bank no longer knows the true identity

When a bank believes that it would no longer be satisfied that it knows the true identity of the account holder.

J. Some examples of suspicious activities/transactions to be monitored by the operating staff-

(i) Large Cash Transactions
(ii) Multiple accounts under the same name
(iii) Frequently converting large amounts of currency from small to large denomination notes
(iv) Placing funds in term Deposits and using them as security for more loans.
(v). Large deposits immediately followed by wire transfers.
(vi). Sudden surge in activity level.
(vii). Same funds being moved repeatedly among several accounts.
(viii). Multiple deposits of money orders, Banker's cheques, drafts of third Parties
(ix). Multiple deposits of Banker's cheques, demand drafts, cross/ bearer.
(x) Cheques of third parties into the account followed by immediate cash withdrawals.
(xi) Transactions inconsistent with the purpose of the account.
(xii) Maintaining a low or overdrawn balance with high activity

Check list for preventing money-laundering activities:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

p. A customer or a non customer receives incoming wire transfers from the Bank to 'Pay upon proper identification' or to convert the funds to bankers' cheques and mail them to the customer or non-customer, when

q. The amount is very large (say over Rs.10 lakhs)
The amount is just under a specified threshold.
The funds come from A foreign country or
Such transactions occur repeatedly.

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

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

2. INDICATIVE LIST OF HIGH RISK CUSTOMERS

i. Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UNSC 1267 & 1988 [2011] linked to Al Qaida & Taliban.
ii. 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
iii. Individuals and entities in watch lists issued by Interpol and other similar international organizations
iv. Customers with dubious reputation as per public information locally available or commercially available.
v. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk
vi. 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.
vii. Customers based in high risk countries/jurisdictions or locations as identified by FATF from time to time.
viii. Politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
ix. Non-resident customers and foreign nationals
x. Accounts of Embassies / Consulates;
xi. Off-shore (foreign) corporation/business
xii. Non face-to-face customers
xiii. High net worth individuals [HNIs]
xiv. Firms with 'sleeping partners'
xv. Companies having close family shareholding or beneficial ownership
xvi. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
xvii. Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence
xviii. Investment Management / Money Management Company/Personal Investment Company
xix. Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the financial institution.
xx. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc
xxi. Trusts, charities, NGOs/NPOs (especially those operating on a “cross-border” basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies)
xxii. Money Service Business: including seller of: Money Orders / Travelers’ Checks / Money Transmission / Check Cashing / Currency Dealing or Exchange
xxiii. Business accepting third party checks (except supermarkets or retail stores that accept payroll checks/cash payroll checks)
xxiv. Gambling/gaming including “Junket Operators” arranging gambling tours

xxv. Dealers in high value or precious goods (e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers).
xxvi. Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries.
xxvii. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
xxviii. Customers that may appear to be Multi level marketing companies etc.

3. INDICATIVE LIST OF MEDIUM RISK CUSTOMERS

i. Non-Bank Financial Institution
ii. Stock brokerage
iii. Import / Export
iv. Gas Station
v. Car / Boat / Plane Dealership
vi. Electronics (wholesale)
vii. Travel agency
viii. Used car sales
ix. Telemarketers
x. Providers of telecommunications service, internet café, IDD call service, phone cards, phone center
xi. Dot-com company or internet business
xii. Pawnshops
xiii. Auctioneers
xiv. Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.
xv. Sole Practitioners or Law Firms (small, little known)
xvi. Notaries (small, little known)
xvii. Secretarial Firms (small, little known)
xviii. Accountants (small, little known firms)
xix. Venture capital companies

4. LIST OF HIGH/MEDIUM RISK PRODUCTS &SERVICES

i. Electronic funds payment services such as Electronic cash (e.g., stored value and payroll cards), funds transfers (domestic and international), etc
ii. Electronic banking
iii. Private banking (domestic and international)
iv. Trust and asset management services
v. Monetary instruments such as Travelers' Cheque
vi. Foreign correspondent accounts
vii. Trade finance (such as letters of credit)
viii. Special use or concentration accounts
ix. Lending activities, particularly loans secured by cash collateral and marketable securities
x. Non-deposit account services such as Non-deposit investment products and Insurance
xi. Transactions undertaken for non-account holders (occasional customers)
xii. Provision of safe custody and safety deposit boxes
xiii. Currency exchange transactions

xiv. Project financing of sensitive industries in high-risk jurisdictions
xv. Trade finance services and transactions involving high-risk jurisdictions
xvi. Services offering anonymity or involving third parties
xvii. Services involving banknote and precious metal trading and delivery
xviii. Services offering cash, monetary or bearer instruments; cross-border transactions, etc.

5. INDICATIVE LIST OF HIGH / MEDIUM RISK GEOGRAPHIES/ LOCATIONS/ COUNTRIES

Countries/Jurisdictions

i. Countries subject to sanctions, embargoes or similar measures in the United Nations Security Council Resolutions ("UNSCR").
ii. Jurisdictions identified in FATF public statement as having substantial money laundering and terrorist financing (ML/FT) risks (www.fatf-gafi.org)
iii. Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies (www.fatf-gafi.org)
iv. Tax havens or countries that are known for highly secretive banking and corporate law practices
v. Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures.
vi. Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
vii. Countries identified by credible sources as having significant levels of criminal activity.
viii. Countries identified by the bank as high-risk because of its prior experiences, transaction history, or other factors (e.g. legal considerations, or allegations of official corruption).

Locations

i. Locations within the country known as high risk for terrorist incidents or terrorist financing activities (e.g. sensitive locations in Jammu and Kashmir, North east, Naxal affected districts)
ii. Locations identified by credible sources as having significant levels of criminal, terrorist, terrorist financing activity.
iii. Locations identified by the bank as high-risk because of its prior experiences, transaction history, or other factors.

6. Indicative List of High Risk Countries:

The countries identified by Financial Action Task Force [FATF] as high risk countries which continue to show deficiencies in their Anti Money Laundering and Combating of Financing of Terrorism framework will be circulated from time to time.

INDICATIVEALERTINDICATORSFORBRANCHES/DEPARTMENTS

S no	Indicative Rule / Scenario
1	CV 1.1 Customer abandoned the transaction for the KYC requirement.
2	CV 2.1 Customer offered false or forged identification documnents.
3	CV 3.1 Address non-existent at the time of account opening.
4	3.2 Address found to be wrong at the time of account opening.
5	CV 4.1 Complex structure created to avoid identification of beneficial owner.
6	LQ 2.1 Customer being investigated for select criminal offences.
7	MR 1.1 Adverse media report for criminal offences
8	MR 2.1 Adverse media report about terrorist activities of customer.
9	EL 1.1 Customer abandoned the transaction when questioned.
10	EL 2.1 Customer body language based alert.
11	EL 2.3 Customer provide inconsistent information.
12	EL 3.1 Customer appears to be acting on behalf while posing in person.
13	EL 4.1 Customer avoiding nearer branches without rationale
14	EL 4.2 Customer offer different identification on different occasions.
15	EL 4.3 Customer purposely wants to avoid reporting.
16	EL 4.4 Customer is not able to explain the source of funds.
17	EL 5.1 Transaction is unnecessarily made to be complex.
18	EL 5.2 Transaction has no economic rationale.
19	EL 5.3 Transaction inconsistent with business / profile.
20	PC 1.1 Complaints received from public
21	BA 1.1 Alerts raised by agent.
22	BA 1.2 Alert raised by other institution.
23	WL1.1 Match with UN list
24	WL1.2 Match with UAPA list
25	WL1.3 Match with MBGB Internal Watch list
26	TM3.1 sudden high value transaction for the client
27	TM3.2 Sudden increase in value of transactions in a month for the client
28	TM4.1 High value txn in new account
29	TM4.2 High activity in a new account

30	TM6.1 High value cash txns inconsistent with profile
31	TY 1.1 - Splitting of cash deposits just below INR 10,00,000 in multiple accounts in a month.
32	TY1.2 Splitting of cash deposits just below INR 50,000.00
33	TY1.5 Frequent low cash deposits
34	TY1.6 Frequent low cash withdrawls
35	TY2.1 Many to one fund transfer
36	TY2.2 one to many fund transfer
37	TY3.1 Customer providing different details to avoid linkage
38	TY5.1 Majority of card repayments in cash
39	TY5.2 Large debit balance in credit card
40	TY7.1 Repayment of loan in cash
41	Ty7.4 Frequent locker operations
42	RM1.2 high value cash txn in NPO
43	RM1.4 High value cash txns by dealer in precious metal or stone
44	RM2.2 High value inward remittance

Annexure III

File No.17015/10/2002-IS-VI
Government of India
Ministry of Home Affairs
Internal Security-I Division

New Delhi, dated 27th August, 2009

ORDER

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

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

"51A. For the prevention of, and for coping with terrorist activities, the Central Government shall have power to –

(a) freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;
(b) prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism;
(c) prevent the entry into or the transit through India of individuals Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism",

The Unlawful Activities (Prevention) Act define "Order" as under:-

"Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as may be amended from time to time.
In order to expeditiously and effectively implement the provisions of Section 51A, the following procedures shall be followed:-

Appointment and Communication of details of UAPA nodal officers

2. As regards appointment and communication of details of UAPA nodal officers –

(i) The UAPA nodal officer for IS-I division would be the Joint Secretary (IS.I), Ministry of Home Affairs. His contact details are 011-23092736(Tel), 011-23092569(Fax) and e-mail.

(ii) The Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, FIU-IND; and RBI, SEBI, IRDA (hereinafter referred to as Regulators) shall appoint a UAPA nodal officer and communicate the name and contact details to the IS-I Division in MHA.

(iii) The States and UTs should appoint a UAPA nodal officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the IS-I Division in MHA.

(iv) The IS-I Division in MHA would maintain the consolidated list of all UAPA nodal officers and forward the list to all other UAPA nodal officers.

(v) The RBI, SEBI, IRDA should forward the consolidated list of UAPA nodal officers to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively.

(vi) The consolidated list of the UAPA nodal officers should be circulated to the nodal officer of IS-I Division of MHA in July every year and on every change. Joint Secretary(IS-I), being the nodal officer of IS-I Division of MHA, shall cause the amended list of UAPA nodal officers to be circulated to the nodal officers of Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, RBI, SEBI, IRDA and FIU-IND.

Communication of the list of designated individuals/entities

3. As regards communication of the list of designated individuals/entities-

(i) The Ministry of External Affairs shall update the list of individuals and entities subject to UN sanction measures on a regular basis. On any revision, the Ministry of External Affairs would electronically forward this list to the Nodal Officers in Regulators, FIU-IND, IS-I Division and Foreigners' Division in MHA.

(ii) The Regulators would forward the list mentioned in (i) above (referred to as designated lists) to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively.

(iii) The IS-I Division of MHA would forward the designated lists to the UAPA nodal officer of all States and UTs.

(iv) The Foreigners Division of MHA would forward the designated lists to the immigration authorities and security agencies.

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

4. As regards funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc., the Regulators would forward the designated lists to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively. The RBI, SEBI and IRDA would issue necessary guidelines to banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies requiring them to -

(i) Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc. with them.

(ii) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc. held by such customer on their books to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail.

(iii) The banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies shall also send by post a copy of the communication mentioned in (ii) above to the UAPA nodal officer of the state/ UT where the account is held and Regulators and FIU-IND, as the case may be.

(iv) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt**,** the banks stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail.

(v) The banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (ii) above , carried through or attempted, as per the prescribed format.

5. On receipt of the particulars referred to in paragraph 3(ii) above, IS-I Division of MHA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/entities identified by the banks, stock exchanges/depositories, intermediaries regulated by SEBI and Insurance Companies are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies are held by the designated individuals/entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

6. In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned bank branch, depository, branch of insurance company branch under intimation to respective Regulators and FIU-IND. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy thereof to all the Principal Secretary/Secretary, Home Department of the States or UTs, so that any individual or entity may be prohibited from making any funds, financial assets or economic assets or economic resources or related services available for the benefit of the designated individuals/entities or any other person engaged in or suspected to be engaged in terrorism. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy of the order under Section 51A, to all Directors General of Police/Commissioners of Police of all states/UTs for initiating action under the provisions of Unlawful Activities (Prevention) Act. The order shall take place without prior notice to the designated individuals/entities.

Regarding financial assets or economic resources of the nature of immovable properties.

7. IS-I Division of MHA would electronically forward the designated lists to the UAPA nodal officer of all States and UTs with the request to have the names of the

designated individuals/entities, on the given parameters, verified from the records of the office of the Registrar performing the work of registration of immovable properties in their respective jurisdiction.

8. In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property and if any match with the designated individuals/entities is found, the UAPA nodal officer of the State/UT would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources of the nature of immovable property to the Joint Secretary (IS.I), Ministry of Home Affairs, immediately within 24 hours at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on **e-mail.**

9. The UAPA nodal officer of the State/UT may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent by the Registrar performing the work of registering immovable properties are indeed of these designated individuals/entities. This verification would be completed within a maximum of 5 working days and should be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual/entity to Joint Secretary(IS-I), Ministry of Home Affairs at the Fax telephone numbers and also on the e-mail id given below.

10. A copy of this reference should be sent to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail**.** MHA may have the verification also conducted by the Central Agencies. This verification would be completed within a maximum of 5 working days.

11. In case, the results of the verification indicate that the particulars match with those of designated individuals/entities, an order under Section 51A of the UAPA would be issued within 24 hours, by the nodal officer of IS-I Division of MHA and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA nodal officer of the State/UT.
The order shall take place without prior notice, to the designated individuals/entities.

12. Further, the UAPA nodal officer of the State/UT shall cause to monitor the transactions/accounts of the designated individual/entity so as to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the schedule to the order or any other person engaged in or suspected to be engaged in terrorism. The UAPA nodal officer of the State/UT shall upon coming to his notice, transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State/UT for also initiating action under the provisions of Unlawful Activities (Prevention) Act.

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

13. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or

at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

14. To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA nodal officer for IS-I Division for freezing of funds or other assets.

15. The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within 5 working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officers in Regulators. FIU-IND and to the nodal officers of the States/UTs. The proposed designee, as mentioned above would be treated as designated individuals/entities.

16. Upon receipt of the requests by these nodal officers from the UAPA nodal officer of IS-I Division, the procedure as enumerated at paragraphs 4 to 12 above shall be followed.

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

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

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

18. The banks stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State/UT nodal officers shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact details given in paragraph 4(ii) above within two working days.

19. The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within 15 working days, unfreezing the funds, financial assets or economic resources or related services,

owned/held by such applicant under intimation to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance company and the nodal officers of States/UTs. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

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

20. All Orders under section 51A of Unlawful Activities (Prevention) Act, relating to funds, financial assets or economic resources or related services, would be communicated to all banks, depositories/stock exchanges, intermediaries regulated by SEBI, insurance companies through respective Regulators, and to all the Registrars performing the work of registering immovable properties, through the State/UT nodal officer by IS-I Division of MHA.

Regarding prevention of entry into or transit through India.

21. As regards prevention of entry into or transit through India of the designated individuals, the Foreigners Division of MHA, shall forward the designated lists to the immigration authorities and security agencies with a request to prevent the entry into or the transit through India. The order shall take place without prior notice to the designated individuals/entities.

22. The immigration authorities shall ensure strict compliance of the Orders and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the Foreigners' Division of MHA.

Procedure for communication of compliance of action taken under Section 51A.

23. The nodal officers of IS-I Division and Foreigners Division of MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities frozen by an order, and details of the individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs for onward communication to the United Nations.

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

(D .Diptivilasa)
Joint Secretary to Government of India