KYC Policy

(With Effect From October 2020)

1. Introduction

The objective of KYC/AML/CFT guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable banks to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. Banks were advised to follow certain customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority. These 'Know Your Customer' guidelines have been revisited in the context of the Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT). Detailed guidelines based on the Recommendations of the Financial Action Task Force and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision, with indicative suggestions wherever considered necessary, have been issued. Banks are advised to ensure that a proper policy framework on 'Know Your Customer' and Anti-Money Laundering measures with the approval of the Board is formulated and put in place. The guidelines issued by the Reserve Bank are under Section 35 A of Banking Regulation Act, 1949 (As Applicable to Co-operative Societies) and any contravention of or non- compliance with the same may attract penalties under the relevant provisions of the Act.

1.1 Definition of Customer

For the purpose of KYC policy, a 'Customer' is defined as:

• a person or entity that maintains an account and/or has a business relationship with the bank;

• one on whose behalf the account is maintained (i.e. the beneficial owner);

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

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

2. Guidelines

2.1 General

(i) Only 'mandatory' information required for KYC purpose which the customer is obliged to give while opening an account at the time of opening the account / during periodic updation. Other 'optional' customer details / additional information, if required, may be obtained separately only after the account is opened with the explicit consent of the customer. The customer has a right to know what is the information required for KYC that she / he is obliged to give and what is the additional information sought by the bank that is optional.

(ii) The information (both 'mandatory' - before opening the account as well as 'optional'- after opening the account with the explicit consent of the customer) collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Banks should, therefore, ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard.

(iii) Any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travellers' cheques for value of Rupees fifty thousand and above is effected by debit to the customer's account or against cheques and not against cash payment.

(iv) The provisions of Foreign Contribution (Regulation) Act, 1976 as amended from time to time, wherever applicable, are strictly adhered to.

2.2 KYC Policy

We have consolidated all such guidelines/instructions for opening of new accounts and effecting transactions therein and the "KYC policy of Jharneshwar Nagrik Sahakari Bank Mydt. has been amended/reviewed.

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

2.3 Customer Acceptance Policy (CAP)

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

(ii) Parameters of risk perception are clearly defined in terms of the nature of Business activity , location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorisation of customers into low, medium and high risk. Customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs) may be categorised n higher risk;

(iii) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and instructions/ guidelines issued by Reserve Bank from time to time;

(iv) Not to open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non cooperation of the ustomer or non reliability of the data/information furnished to the bank. Decision to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision;

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

(vi) Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organisations etc.

b) The increasing complexity and volume of financial transactions necessitate that customers do not have multiple identities within the bank, across the banking system and across the financial system. This can be achieved by introducing a unique identification code for each customer. In this regard, a Working Group constituted by the Government of India has proposed the introduction of unique identifiers for customers across different banks and Financial Institutions

for setting up a centralized KYC Registry. Unique Customer Identification Code (UCIC) to be allotted to all the customers while entering into any new relationships for individual customers. Similarly, existing individual customers should be allotted unique customer identification code. The UCIC will help to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers. It would also smoothen banking operations for the customers.

c) A profile for each new customer should be prepared based on risk categorisation. The customer profile may 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. However, while preparing customer profile it should be taken care to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein should not be divulged for cross selling or any other purposes.

d) For the purpose of risk categorisation, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorised as **low risk**. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. NPOs/NGOs promoted by United Nations or its agencies may be classified as low risk customer. NPOs/NGOs promoted by United Nations or its agencies may be classified as low risk customer.

Customers that are likely to pose a higher than average risk to the bank should be categorised as **medium or high risk** depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Banks should apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. Examples of customers requiring higher due diligence include (a) nonresident customers; (b) high net worth individuals; (c) trusts, charities, NGOs and organizations receiving donations; (d) companies having close family shareholding or beneficial ownership; (e) firms with 'sleeping partners'; (f) politically exposed persons (PEPs) of foreign origin; (g) non-face to face customers and (h) those with dubious reputation as per public information available etc.

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

2.4 Customer Identification Procedure (CIP)

(a) Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Branch need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship. Being satisfied means that the bank must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based approach is considered necessary to avoid

disproportionate cost to banks and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.). For customers that are natural persons, the branches should obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the branch should (i) verify the legal status of the legal person/entity through proper and relevant documents; (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorised and identify and verify the identity of that person; (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in paragraph 2.5 below for guidance. Reasonable measures should be taken to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows Who the beneficial owner(s) is/are:

(b) Rule 9(1A) of the Prevention of Money Laundering Rules, 2005 requires that every banking company, and financial institution, as the case may be, shall identify the beneficial owner and take all reasonable steps to verify his identity. The term "beneficial owner" has been defined as the natural person who ultimately owns or controls a client and / or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person. Government of India has since examined the issue and has specified the procedure for determination of Beneficial Ownership. The procedure as advised by the Government of India is as under:

A. Where the client is a person other than an individual or trust, the banking company and financial institution, as the case may be, shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

(i) The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

> Explanation : Controlling ownership interest means ownership of / entitlement to more than 25 percent of shares or capital or profits of the juridical person, where the juridical person is a company; ownership of / entitlement to more than 15% of the capital or profits of the juridical person where the juridical person is a partnership; or, ownership of / entitlement to more than 15% of the property or capital or profits of the juridical person where the juridical person is an unincorporated association or body of individuals.

(ii) In cases where there exists doubt under (i) as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership Interests, the identity of the natural person exercising control over the juridical person through other means.

> Explanation: Control through other means can be exercised through voting rights, agreement, arrangements, etc.

(iii) Where no natural person is identified under (i) or (ii) above, the identity of the relevant natural person who holds the position of senior managing official.

B. Where the client is a trust, the banking company and financial institution, as the case may be, shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, 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.

C. Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

(c) It has been observed that some close relatives, e.g. wife, son, daughter and daughter and parents etc. who live with their husband, father/mother and son, as the case may be, are finding it difficult to open account in some banks as the utility bills required for address verification are not in their name. It is clarified, that in such cases, branches can obtain an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) wanting to open an account is a relative and is staying with him/her. Any supplementary evidence such as a letter received through post for further verification of the address can be used.

(d) Periodical updation of customer identification data (including photograph/s) be updated after the account is opened. The periodicity of such updation should be as follows

(i) Full KYC exercise will be required to be done at least every two years for **high risk** individuals and entities.

(ii) Full KYC exercise will be required to be done at least every eight years for **medium risk** and at least every ten years for low risk individuals and entities.

(iii) Positive confirmation (obtaining KYC related updates through e-mail / letter / telephonic conversation / forms / interviews / visits, etc.), will be required to be completed at least every two years for medium risk and at least every three years for **low risk** individuals and entities.

(iv) Fresh photographs will be required to be obtained from minor customers on their becoming major.

On-going due diligence to be carried out with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and, wherever necessary, the source of funds.

(e) An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in Annex I . It is clarified that permanent correct address, as referred to in Annex I, means the address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other document for verification of the address of the customer. It is clarified that while opening accounts based on Aadhaar the branch should satisfy themselves about the current address of the customer by obtaining required proof of the same as per extant instructions.

2.5 Customer Identification Requirements – Indicative Guidelines

(i) Trust/Nominee or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. If a customer is acting on behalf of another person as trustee/nominee or any other intermediary, receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting be obtained, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, reasonable precautions are to be taken to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

(ii) Accounts of companies and firms

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

(b) Certain firms posing as Multi Level Marketing (MLM) agencies for consumer goods and services have been mobilizing large deposits from the public (with promise of high return) by opening accounts at various bank branches. These funds running into crores of rupees were being pooled at the principal accounts of the MLM Firms and were eventually flowing out of the accounts for purpose appearing illegal or highly risky. Accordingly, while opening agency accounts in the name of a proprietary concern the following documents need to be obtained and verified.

(i) Identity as also the address proof of the proprietor, such as passport, PAN card, Voter ID card, Driving Licence, Ration Card with photo, etc. – any one of the document is obtained.

(ii) Proof of the name, address and activity of the concern, like registration certificate(in the case of a registered concern), certificate / licence issued by the Municipal authorities under Shop and Establishment act, sales and income tax returns, CST / VAT certificate, Licence issued by the registering authority like Certificate of Practice issued by the Institute of Chartered Accountants of India, Institute of Companies Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, any certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, etc. **any two of the documents** are to be obtained. These documents should be in the name of the proprietary concern. Further, the complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated /acknowledged by the Income Tax Authorities and utility bills such as electricity, water and landline telephone bills in the name of the proprietary concern are also included in the indicative list of required documents for opening accounts of proprietary concerns.

(vi) Opening of bank accounts – Salaried Employees : It has been brought to our notice that for opening bank accounts of salaried employees, it is necessary to rely on such certification

only from corporates and other entities of repute and should be aware of the competent authority designated by the concerned employer to issue such certificate/letter. Further, **in addition** to the certificate from employer, at least one of the officially valid documents as provided in the Prevention of Money Laundering Rules (viz. passport, driving licence, PAN Card, Voter's Identity card etc.) or utility bills for KYC purposes for opening bank account of salaried employees of corporates and other entities be obtained.

(vii) Opening of new accounts - Proof of identity and address

For complying with KYC requirements for opening new accounts, it is clarified that :

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

(b) If the address indicated on the document submitted for identity proof differs from the current address mentioned in the account opening form, a separate proof of address should be obtained. For this purpose, apart from the indicative documents listed in Annex I of this policy, a rent agreement indicating the address of the customer duly registered with State Government or similar registration authority may also be accepted as a proof of address.

(viii) Introduction not Mandatory for opening accounts

Since introduction is not necessary for opening of accounts under PML Act and Rules or Reserve Bank's extant KYC instructions, branches should not insist on introduction for opening bank accounts of customers.

(ix) Acceptance of Aadhaar letter / e-KYC service (on-line Aadhaar authentication) of UIDAI for KYC purposes

a) Physical Aadhaar card / letter issued by UIDAI containing details of name, address and Aadhaar number received through post should be accepted as an 'Officially Valid Document'. Unique Identification Authority of India (UIDAI) has advised Reserve Bank that banks are accepting Aadhaar letter issued by it as a proof of identity but not of address, for opening accounts. As indicated at paragraph 2.5 (vii) above, if the address provided by the account holder is the same as that on Aadhaar letter, it may be accepted as a proof of both identity and address.

b) Further, in order to reduce the risk of identity fraud, document forgery and have paperless KYC verification, UIDAI has launched its e-KYC service. Accordingly, it has been decided to accept e-KYC service as a valid process for KYC verification under Prevention of Money Laundering (Maintenance of Records) Rules, 2005. The information containing demographic details and photographs made available from UIDAI as a result of e-KYC process ("which is in an electronic form and accessible so as to be usable for a subsequent reference") may be treated as an 'Officially Valid Document' under PML Rules. In this connection, it is advised that while using e-KYC service of UIDAI, the individual user has to authorize the UIDAI, by explicit consent, to release her or his identity / address through biometric authentication to the bank branches. The broad operational instructions to banks on Aadhaar e-KYC service are enclosed as Annex V.

c) Alternatively, e-Aadhaar downloaded from UIDAI website may be accepted as an officially valid document subject to the following:

i) If the prospective customer knows only his / her Aadhaar number, the UCB may print the prospective customer's e-Aadhaar letter in the UCB directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in the paragraph 2.5 (ix) (b) above.

ii) If the prospective customer carries a copy of the e-Aadhaar downloaded elsewhere, the UCB may print the prospective customer's e-Aadhaar letter in the UCB directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in the paragraph 2.5 (ix) (b) above; or confirm identity and address of the resident through simple authentication service of UIDAI.

(x) Acceptance of NREGA Job Card as KYC for normal accounts

In order to avoid inconvenience to customers from rural areas, branches are advised that they may now accept NREGA Job Card as an 'officially valid document' for opening of bank accounts without the limitations applicable to 'Small Accounts'.

(xi) Shifting of bank accounts to another centre - Proof of address

KYC once done by one branch of the bank should be valid for transfer of the account within the bank as long as full KYC procedure had been done for the concerned account. The customer should be allowed to transfer his account from one branch to another branch without restrictions. However, it has been brought to our notice that a large number of customers with transferable jobs or those who migrate for jobs are unable to produce a proof of current / permanent address while opening a bank account immediately after relocating. In view of this, it is clarified that

(a) Henceforth, customers may submit only one documentary proof of address (either current or permanent) while opening a bank account or while undergoing periodic updation. In case the address mentioned as per 'proof of address' undergoes a change, fresh proof of address may be submitted to the branch within a period of six months.

(b) In case the proof of address furnished by the customer is not the local address or address where the customer is currently residing, the UCB may take a declaration of the local address on which all correspondence will be made by them with the customer. No proof is required to be submitted for such address for the purpose of correspondence. This address may be verified by the bank through 'positive confirmation' such as acknowledgment of receipt of (i) letters, cheque books, ATM card, (ii) telephonic conversation, (iii) visits etc. In the event of change in this address due to relocation or any other reason/s, customers may intimate the new address for correspondence to the UCB within two weeks of such a change.

While opening new accounts and while periodically updating KYC data as required in terms of paragraph 2.4 (d) of this Master Circular, an undertaking to this effect should be obtained. In all these cases customers will have to produce proof of address as mentioned at (a) and (b) above.

(xii) Opening of Savings Bank Accounts and Credit Linking of account for Self Help Groups (SHGs)

In order to address the difficulties faced by Self Help Groups (SHGs) in complying with KYC norms while opening savings bank accounts and credit linking of their accounts, it is clarified that 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, it is clarified that since KYC would have already been verified while opening the savings bank account and the account continues to be in operation and is to be used for credit linkage, no separate KYC verification of the members or office bearers is necessary.

2.6 Small Deposit Accounts

(i) Although flexibility in the requirements of documents of identity and proof of address has been provided in the above mentioned KYC guidelines, it has been observed that a large number of persons, especially, those belonging to low income group both in urban and rural areas are not able to produce such documents to satisfy the branch about their identity and address. This would lead to their inability to access the banking services and result in their financial exclusion. Accordingly, the KYC procedure also provides for opening accounts for those persons who intend to keep balances not exceeding Rupees Fifty Thousand (Rs. 50,000.00) in all their accounts taken together and the total credit in all the accounts taken together is not expected to exceed Rupees One Lakh (Rs. 1,00,000.00) in a year. In such cases, if a person who wants to open an account and is not able to produce documents mentioned in Annex I of this Master Circular, branches should open an account for him, subject to any evidence as to the identity and address of the customer to the satisfaction of the branch.

(ii) While opening accounts as described above, the customer should be made aware that if at any point of time, the balances in all his/her accounts with the bank (taken together) exceeds Rupees Fifty Thousand (Rs. 50,000.00) or total credit in the account exceeds Rupees One Lakh (Rs. 1,00,000.00) in a year, no further transactions will be permitted until the full KYC procedure is completed. In order not to inconvenience the customer, the branch must notify the customer when the balance reaches Rupees Forty Thousand (Rs. 40,000.00) or the total credit in a year reaches Rupees Eighty thousand (Rs. 80,000.00) that appropriate documents for conducting the KYC must be submitted otherwise operations in the account will be stopped.

(iii) In terms of Government of India, Notification No. 14/2010/F.No.6/2/2007-E.S dated December 16, 2010, the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 has been amended.

A.Small Accounts:

a) In terms of Rule 2 clause (fb) of the Notification 'small account' means a savings account in a banking company where-

(i) The aggregate of all credits in a financial year does not exceed rupees one lakh;
(ii) The aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and
(iii) The balance at any point of time does not exceed rupees fifty thousand.

b) Rule (2A) of the Notification lays down the detailed procedure for opening 'small accounts'. Branches are advised to ensure adherence to the procedure provided in the Rules for opening of small accounts.

c) Branches are advised to open 'Small Accounts' for all persons who so desire. It is reiterated that all limitations applicable to 'Small Accounts' should be strictly observed.

B. Officially valid documents

The Notification has also expanded the definition of 'officially valid document' as contained in clause (d) of Rule 2(1) of the PML Rules to include job card issued by NREGA duly signed by

an officer of the State Government or the letters issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number. In addition, documents obtained through e-KYC service of UIDAI as detailed in para 2.5 (ix) above may also be accepted as an 'officially valid document'.

2.7 Monitoring of Transactions

(i) Ongoing monitoring is an essential element of effective KYC procedures. Branches can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. Branches should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Branches may pay particular attention to particular category of accounts about the transactions. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the branch. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts have to be subjected to intensified monitoring. Bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. Branches should follow the system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers should be carried out at a periodicity of **not less** than once in six months. Banks are also required to put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorisation and updated profile of customers. It is needless to add that a robust software throwing alerts is essential for effective identification and reporting of suspicious transactions.

(ii) In view of the risks involved in cash intensive businesses, accounts of bullion dealers (including sub-dealers) & Jewellers should also be categorised by banks as "**high risk**" requiring enhanced due diligence.

(iii) It is advised that high risk associated accounts should be taken into account to identify Suspicious Transactions Reports.

2.8 Closure of accounts

Where the branch is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the branch should consider closing the account or terminating the banking/business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken by the Branch Manager.

2.9 Risk Management

(a)It should cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility should be explicitly allocated within the bank for ensuring that the bank's policies and procedures are implemented effectively. Banks should, in consultation with their boards, devise procedures for creating risk profiles of their existing and new customers and apply various anti money laundering measures keeping in view the risks involved in a transaction, account or banking/business relationship.

(b) The internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. Concurrent/ Internal Auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard should be put up before the Audit Committee of the Board on quarterly intervals.

2.11 Usage of 'At par' Cheque facility extended to Cooperative Banks by Scheduled Commercial Banks

'At par' cheque facility can be utilized only for the following purposes:

i) for our own use.

ii) for the account holders who are KYC compliant provided that all transactions of `50,000.00 or more should be strictly by debit to the customer's account.

iii) for walk-in customers against cash for less than `50,000.00 per individual.

In order to utilise the 'at par' cheque facility in the above manner, the following records are to be maintained:

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.

It should be ensured that all 'at par' cheques issued are crossed 'account payee' irrespective of the amount involved.

It is advised to make use of more efficient means of remittances for the customers like NEFT or RTGS by providing such services directly or by becoming sub-members of banks providing such services as per regulations in this regard issued by RBI from time to time

2.12 Combating Financing of Terrorism

(a) In terms of PMLA Rules, suspicious transaction should include *inter alia* transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. Enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority is advised.

(b) The consolidated list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) received from Government of India circulated by Reserve Bank of India through their circulars are to be updated. List of such individuals/entities can also be accessed in the United Nations website at http://www.un.org/sc/committees/1267/consolist.shtml. The UN Security Council has adopted Resolutions 1988 (2011) and 1989 (2011) which have resulted in splitting of the Consolidated List into two separate lists, namely:

(i) 'Al-Qaida Sanctions List' which is maintained by the 1267 / 1989 Committee. This List shall include only the names of those individuals, groups, undertakings and entities associated with Al-Qaida. General information on the work of the committee is available at

http://www.un.org/sc/committees/1267/information.shtml. The Updated Al-Qaida Sanctions List is available at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml

(ii) '1988 Sanctions List', which is maintained by the 1988 Committee. This list consists of names previously included in Sections A ("Individuals associated with the Taliban") and B ("Entities and other groups and undertakings associated with the Taliban") of the Consolidated List. The Updated 1988 Sanctions list is available at http://www.un.org/sc/committees/1988/list.shtml

It may be noted that both 'Al-Qaida Sanctions List' and '1988 Sanctions List' are to be taken into account for the purpose of implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967. It should be ensured that the name/s of the proposed customer does not appear in either list. Further, all the existing accounts are to be scanned to ensure that no account is held by or linked to any of the entities or individuals included in the two lists. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to the Reserve Bank and FIU-IND.

(c) The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has since issued an Order dated August 27, 2009 detailing the procedure for implementation of Section 51 A of the UAPA relating to the purposes of prevention of, and for coping with terrorist activities. In terms of Section 51 A, 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.

It is advised to strictly follow the procedure laid down in the UAPA Order dated August 27, 2009 (Annex III) and ensure meticulous compliance to the Order issued by the Government.

It is advised that on receipt of the list of individuals and entities subject to UN sanctions (referred to as designated lists) from the Reserve Bank, Bank should ensure expeditious and effective implementation of the procedure prescribed under Section 51 A of UAPA in regard to freezing /unfreezing of financial assets of the designated individuals/entities enlisted in the UNSCRs and especially in regard to funds, financial assets or economic resources or related services held in the form of bank accounts. In terms of paragraph 4 of the Order, in regard to funds, financial assets or economic resources or related services held in the form of bank accounts, the list forwarded by the Reserve Bank should be updated

(i) 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 with us

(ii) In case, the particulars of any of our customers match with the particulars of designated individuals/entities, the branches 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, held by such customer to the Joint Secretary (IS-I), Ministry of Home Affairs (MHA) 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) A copy of the communication mentioned in (ii) above should be sent by post to the UAPA nodal officer of the Reserve Bank, Chief General Manager, Department of Banking Operations and Development, Anti Money Laundering Division, World Trade Centre, 4th Floor, Centre 1, Cuffe Parade, Colaba, Mumbai - 400 005 and also by FAX at No. 022-22185792. The particulars apart from being sent by post/FAX should necessarily be conveyed on e-mail.

(iv) A copy of the communication mentioned in (ii) above should be sent to the UAPA nodal officer of the State/Union Territory where the account is held as the case may be and to FIU-IND.

(v) In case, the match of any of the customers with the particulars of designated individuals/entities is **beyond doubt**, it should be prevented from conducting financial transactions, under intimation to Joint Secretary (IS-I), MHA at Fax No. 011 – 23092569 and also convey over telephone over 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail.

(vi) Suspicious Transaction Report (STR) with FIU-IND should be filed covering all transactions in the accounts covered by paragraph (ii) above, carried through or attempted, as per the prescribed format.

(d) Freezing of financial assets

(i) On receipt of the particulars as mentioned in paragraph c (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 are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by banks are held by the designated individuals/entities. This verification would be completed within a period not exceeding five working days from the date of receipt of such particulars.

(ii) 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 51 A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the bank branch concerned under intimation to the Reserve Bank and FIU-IND.

(iii) The Order shall take place without prior notice to the designated individuals/entities.

(e) Implementation of requests received from foreign countries under UNSCR 1373 of 2001 :

(i) UNSCR 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 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.

(ii) To give effect to the requests of foreign countries under UNSCR 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.

(iii) The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within five 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 the Reserve Bank. The proposed designee, as mentioned above would be treated as designated individuals/entities.

(iv) Upon receipt of the requests from the UAPA nodal officer of IS-I Division, the list would be forwarded to banks and the procedure as enumerated at paragraphs 2.12(c), (d) shall be followed.

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

(f) 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

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 bank concerned. The banks 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 c (ii) above within two working days. 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 fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the bank concerned. 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.

2.15 Principal Officer

(a) Banks should appoint a senior management officer to be designated as Principal Officer. Principal Officer shall be located at the head/corporate office of the bank and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism. With a view to enable the Principal Officer to discharge his responsibilities, it is advised that the Principal Officer and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records and other relevant information. Further, banks should ensure that the Principal Officer is able to act independently and report directly to the senior management or to the Board of Directors.

(b) The Principal Officer will be responsible for timely submission of CTR, STR and reporting of counterfeit notes to FIU-IND.

(c) The Principal Officer will also oversee and ensure overall compliance with regulatory guidelines on KYC / AML / CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made there under, as amended from time to time.

2.17 Maintenance of records of transactions/Information to be preserved/Maintenance and preservation of records/Cash and Suspicious transactions reporting to Financial Intelligence Unit- India (FIU-IND)

Government of India, Ministry of Finance, Department of Revenue, vide its notification dated July 1, 2005 in the Gazette of India, has notified the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the said Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts certain obligations on the banking companies in regard to preservation and reporting of customer account information.

(i) Maintenance of records of transactions

Proper system to be introduced for maintaining proper record of transactions prescribed under Rule 3, as mentioned below:

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

(b) all series of cash transactions integrally connected to each other which have been valued below Rupees Ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten lakh;

(c) 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

(d) all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

Explanation - Integrally connected cash transactions referred to at (b) above

The following transactions have taken place in a branch during the month of April 2008:

Date	**Mode**	**Dr (**Rs.**)**	**Cr (**Rs.**)**	**Balance (**Rs.**) BF – 8,00,000.00**
02/04/2008	Cash	5,00,000.00	3,00,000.00	6,00,000.00
07/04/2008	Cash	40,000.00	2,00,000.00	7,60,000.00
08/04/2008	Cash	4,70,000.00	1,00,000.00	3,90,000.00
Monthly summation		**10,10,000.00**		**6,00,000.00**

As per above clarification, the debit transactions in the above example are integrally connected cash transactions because total cash debits during the calendar month exceeds Rs. 10 lakh. However, the bank should report only the debit transaction taken place on 02/04 and 08/04/2008. The debit transaction dated 07/04/2008 should not be separately reported by the bank, which is less than Rs. 50, 000.00 (Rupees Fifty Thousand). All the credit transactions in the above example would not be treated as integrally connected, as the sum total of the credit transactions during the month does not exceed Rs. 10 lakh and hence credit transaction dated 02, 07 & 08/04/2008 should not be reported by banks.

(ii) Information to be maintained : The following informations are required to be maintained, including necessary information required for reconstruction of the transactions referred to in Rule 3:

(a) the nature of the transactions ;

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

(c) the date on which the transaction was conducted; and

(d) the parties to the transaction

(iii) Maintenance and Preservation of record

(a) It is required to maintain the records (hard and soft copies) containing information in respect of transactions referred to in Rule 3 above. Appropriate steps are to be taken 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. It is to be ensured to maintain for at least ten 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.

(b) It is to be ensured that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least ten years **after the business relationship is ended**. The identification records and transaction data should be made available to the competent authorities upon request.

(c) In paragraph 2.7 of this Master Circular, it is advised 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. It is further clarified that 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 in their day-to-day work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities. These records are required to be preserved for ten years is required under PMLA,2002.

(iv) Reporting to Financial Intelligence Unit – India

(a) In terms of the PMLA rules, banks are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

Director, FIU-IND, Financial Intelligence Unit-India, 6th Floor, Hotel Samrat, Chanakyapuri, New Delhi-110021. Website - http://fiuindia.gov.in/

(b) All the reporting formats should be carefully go through. There are altogether eight reporting formats, as detailed in Annex II, viz. i) Cash Transactions Report (CTR); ii) Summary of CTR iii) Electronic File Structure-CTR; iv) Suspicious Transactions Report (STR); v) Electronic File Structure-STR; vi) Counterfeit Currency Report (CCR); vii) Summary of CCR and viii) Electronic File Structure-CCR.

The reporting formats contain detailed guidelines on the compilation and manner/procedure of submission of the reports to FIU-IND. It would be necessary for banks to initiate urgent steps to ensure electronic filing of all types of reports to FIU-IND. The related hardware and technical requirement for preparing reports in an electronic format, the related data files and data structures thereof are furnished in the instructions part of the concerned formats.

(c) The FIU-India has advised that the above mentioned multiple data files/reporting format is being replaced by a new single XML file format and prepared a comprehensive reporting format guide giving the specifications of the prescribed reports to be furnished to FIU-India. The reporting formats specified in the reporting format guide are: (i) Account based reporting format (ARF) for reporting of account based CTRs, STRs and NTRs (ii) Transactions based reporting format (TRF) for reporting of transaction based CTRs, STRs and NTRs and (iii) CCR reporting format (CRF) for reporting of counterfeit currency reports (CCRs)
(e) FIU-IND has developed a Report Generation Utility and Report Validation Utility to assist reporting entities in the preparation of the prescribed reports. Reporting entities, which have necessary technical capabilities, may generate XML reports directly from their systems. Reporting entities are encouraged to shift to the fixed width data structure version 2.0 before generating XML reports at their end.

The following documents have been placed in the 'Downloads' section of the FIU-IND website (http://fiuindia.gov.in).

(i) Reporting Format Guide

(ii) XML Schemas: AccountBasedReport.xsd, TransactionBasedReport.xsd, CCRBasedReport.xsd, FIU-INDSchemaLibrary.xsd and DataQualityReport.xsd

(iii) User Guides: Report Generation Utility User Guide and Report Validation Utility User Guide

It is advised to carefully go through the reporting formats and initiate urgent steps to build capacity to generate reports, which are compliant with the XML format specifications. The date of transition from the old reporting format to the new reporting format will be communicated to the reporting entities separately.

(v) In terms of instructions contained in paragraph 2.3 (c) of this Master Circular, it is required to prepare a profile for each customer based on risk categorisation. Further, vide paragraph 2.7, the need for periodical review of risk categorisation has been emphasized. It is, therefore,

reiterated that banks, as a part of transaction monitoring mechanism, are required to put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers. It is needless to add that a robust software throwing alerts is essential for effective identification and reporting of suspicious transaction.

(vi) The CEOs should personally monitor the adherence by the bank officials to the provisions of the AML/ PMLA guidelines and ensure that systems and procedures are put in place and instructions percolated to the operational levels. It should also be ensured that there is a proper system of fixing accountability for serious lapses and intentional circumvention of prescribed procedures and guidelines.

2.18 Cash and Suspicious Transaction Reports

1. Cash Transaction Report (CTR)

While detailed instructions for filing all types of reports are given in the instructions part of the related formats, banks should scrupulously adhere to the following:

(i) The Cash Transaction Report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month. Cash transaction reporting by branches to their Principal Officer / controlling offices should, therefore, invariably be submitted on monthly basis **(not on fortnightly basis)** and banks should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule. In regard to CTR the cut off limit of Rs. 10 lakh is applicable to integrally connected cash transactions also.

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

(iii) While filing CTR, details of individual transactions below Rupees Fifty thousand need not be furnished.

(iv) CTR should contain only the transactions carried out by the bank on behalf of their clients/customers excluding transactions between the internal accounts of the bank.

(v) A summary of cash transaction report for the bank as a whole should be compiled by the Principal Officer of the bank every month in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted to FIU-India.

(vi) In case of Cash Transaction Reports (CTR) compiled centrally by banks for the branches having Core Banking Solution (CBS) at their central data centre level, banks may generate centralised Cash Transaction Reports (CTR) in respect of branches under core banking solution at one point for onward transmission to FIU-IND, provided:

(a) The CTR is generated in the format prescribed by Reserve Bank in Para 2.17 (iv) (b) of this Master Circular.

(b) A copy of the monthly CTR submitted on its behalf to FIU-India is available at the concerned branch for production to auditors/inspectors, when asked for; and

(c) The instruction on ‘Maintenance of records of transactions’; ‘Information to be preserved’ and ‘Maintenance and Preservation of records’ as contained above in this master circular at paragraph 2.17 (i), (ii) and (iii) respectively are scrupulously followed by the branch.

2. Suspicious Transaction Reports (STR)

(i) While determining suspicious transactions, it should be guided by definition of suspicious transaction 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. It is clarified that banks should report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

(iii) STRs should be made if there is reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

(iv) As per extant instructions, a branch should not open an account (or should consider closing an existing account) when it is unable to apply appropriate CDD measures. It is clarified that in the circumstances when a branch believes that it would no longer be satisfied that it knows the true identity of the account holder, the branch should also file an STR.

(v) The Suspicious Transaction Report (STR) should be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report should be made available to the competent authorities on request.

(vi) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, banks may consider the indicative list of suspicious activities contained in Annex E of the 'IBA's Guidance Note for Banks, 2005'.

(vii) Banks should not put any restrictions on operations in the accounts where an STR has been made. Moreover, it should be ensured that there is no **tipping off to** the customer at any level.

2.19 Maintenance of Records in respect of Non-Profit Organisations and filing of Non-Profit Organisation Transaction Reports (NTRs) to FIU-IND

In view of the Government of India Notification No.13/2009/F.No.6/8/2009-ES dated November 12, 2009 amending the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005, it is required to maintain proper record of all transactions involving receipts by non- profit organizations of value more than rupees ten lakh or its equivalent in foreign currency and to forward a report to FIU-IND of all such transactions in the prescribed format every month by the 15th of the succeeding month. These records are to be maintained for a period of ten years from the date of transactions.

2.20 Maintenance of Records and filing of Suspicious Transaction Reports (STRs) to FIU-IND in respect of Walk-in Customers

Transactions carried out by a non-account based customer, that is a walk-in customer, where the amount of transaction is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified. Further, if a bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000.00 (Rupees Fifty Thousand) the bank should verify identity and address of the customer and also consider filing a suspicious transaction report (STR) to FIU-IND.

2.21 Customer Education/Employee's Training/Employee's Hiring

(a) Customer Education : Implementation of KYC procedures requires branches to demand certain information from customers which may be of personal nature or which have hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. There is, therefore, a need for banks to prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the KYC programme. The front desk staff needs to be specially trained to handle such situations while dealing with customers.

(b) Employee's Training :-Banks must have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements should have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

(c) Hiring of Employees : It may be appreciated that KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking channels. It would, therefore, be necessary that adequate screening mechanism is put in place by banks as an integral part of their recruitment/hiring process of personnel.

Annex I

(Paragraphs No. 2.4, 2.5 & 2.6)

Customer Identification Procedure Features to be verified and documents that may be obtained from customers

Features	Documents
Accounts of individuals • Legal name and any other names used • Correct permanent address	(i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving licence(v) Identity card (subject to the bank's satisfaction) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of bank (vii) Job cards issued by NREGA duly signed by an officer of the State Government (viii) The Letter issued by the Unique Identification Authority of India (UIDAI) or documents obtained through e-KYC service of UIDAI containing details of name, address and Aadhaar number or any other document as notified by the Central Government in consultation with the Reserve Bank of India or any other document as may be required by the banking companies or financial institution or intermediary (i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority(iv) Electricity bill (v) Ration card(vi) Letter from employer (subject to satisfaction of the bank) [(1) Any one document which provides customer information to the satisfaction of the bank will suffice. (2) If the address on the document submitted for identity proof by the prospective customer is same as that declared by him/her in the account opening form, the document may be accepted as a valid proof of both identity and address.]
Accounts of companies • Name of the company	(i) Certificate of incorporation and Memorandum & Articles of Association (ii) Resolution of the Board of Directors to
• Principal place of business • Mailing address of the company • Telephone/Fax Number	open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf (iv) Copy of PAN allotment letter (v) Copy of the telephone bill
Accounts of partnership firms • Legal name • Address • Names of all partners and their addresses • Telephone numbers of the firm and partners	(i) Registration certificate, if registered(ii) Partnership deed (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses (v) Telephone bill in the name of firm/partners

Accounts of trusts & foundations • Names of trustees, settlers , beneficiaries and signatories • Names and addresses of the founder, the managers/directors and the beneficiaries • Telephone/fax numbers	(i) Certificate of registration, if registered (ii) Power of Attorney granted to transact business on its behalf (iii) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses(iv) Resolution of the managing body of the foundation/association(v) Telephone bill

Annex II

(Paragraph No. 2.17 (iv) (b)) (List of various reports)

1. Cash Transaction Report(CTR)
2. Summary of CTR
3. electronic File Structure – CTR
4. Suspicious Transactions Report(STR)
5. Electronic File Structure – STR
6. Counterfeit Currency Report (CCR)
7. Summary of CCR
8. Electronic File Structure - CCR

Annex V

(Paragraph 2.5 (ix) (b) & (c) and 2.6 (B))

Operational Procedure to be followed by UCBs for e-KYC exercise

The e-KYC service of the UIDAI is to be leveraged by UCBs through a secured network. Any UCB willing to use the UIDAI e-KYC service is required to sign an agreement with the UIDAI. The process flow to be followed is as follows :

1. Sign KYC User Agency (KUA) agreement with UIDAI to enable the UCB to specifically access e-KYC service.

2. UCBs to deploy hardware and software for deployment of e-KYC service across various delivery channels. These should be Standardisation Testing and Quality Certification (STQC) Institute, Department of Electronics & Information Technology, Government of India certified biometric scanners at bank branches / micro ATMs / BC points as per UIDAI standards. The current list of certified biometric scanners is given in the link below :

http://www.stqc.gov.in/sites/upload_files/stqc/files/UID_Auth_Certlist_250613.pdf

3. Develop a software application to enable the use of e-KYC across various Customer Service Points (CSP) (including bank branches, BCs etc.) as per UIDAI defined Application Programming Interface (API) protocols. For this purpose UCBs will have to develop their own software under the broad guidelines of UIDAI. Therefore, the software may differ from UCB to UCB.

4. Define a procedure for obtaining customer authorization to UIDAI for sharing e-KYC data with the UCB. This authorization can be in physical (by way of a written explicit consent authorising UIDAI to share his / her Aadhaar data with the UCB / BC for the purpose of opening bank account) / electronic form as defined by UIDAI from time to time.

5. Sample process flow would be as follows :

a. Customer walks into CSP of a UCB with his / her 12-digit Aadhaar number and explicit consent and requests to open a bank account with Aadhaar based e-KYC.

b. UCB representative manning the CSP enters the number into bank's e-KYC application software.

c. The customer inputs his / her biometrics via a UIDAI compliant biometric reader (e.g. fingerprints on a biometric reader).

d. The software application captures the Aadhaar number along with biometric data, encrypts this data and sends it to UIDAI's Central Identities Data Repository (CIDR).

e. The Aadhaar KYC service authenticates customer data. If the Aadhar number does not match with the biometrics, UIDAI server responds with an error with various reason codes depending on type of error (as defined by UIDAI).

f. If the Aadhaar number matches with the biometrics, UIDAI responds with digitally signed and encrypted demographic information [Name, year / date of birth, Gender, Address, Phone and email (if available)] and photograph. This information is captured by UCB's e-KYC application and processed as needed.

g. UCB's servers auto populate the demographic data and photograph in relevant fields. It also records the full audit trail of e-KYC viz. source of information, digital signatures, reference number, original request generation number, machine ID for device used to generate the request, date and time stamp with full trail of message routing, UIDAI encryption date and time stamp, UCB's decryption date and time stamp, etc.

h. The photograph and demographics of the customer can be seen on the screen of computer at bank branches or on a hand held device of BCs for reference.

i. The customer can open bank account subject to satisfying other account opening requirements.

Manager General Manager