भारतीय रिजर्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2015-16/108
DNBR (PD) CC No. 051/03.10.119/2015-16 **July 1, 2015**

To

All Non-Banking Financial Companies (NBFCs),
Miscellaneous Non-Banking Companies (MNBCs),
and Residuary Non-Banking Companies (RNBCs)

Dear Sir/Madam,

Master Circular – 'Know Your Customer' (KYC) Guidelines – Anti Money Laundering Standards (AML) -'Prevention of Money Laundering Act, 2002 - Obligations of NBFCs in terms of Rules notified thereunder'

As you are aware, in order to have all current instructions on the subject at one place, the Reserve Bank of India issues updated circulars / notifications. The instructions related to the captioned subject contained in various circulars issued by RBI updated as on June 30, 2015 are reproduced below. The updated circular has also been placed on the RBI web-site (https://www.rbi.org.in).

Yours faithfully,

(C. D. Srinivasan)
Chief General Manager

गैर बैंकिंग विनियमन विभाग , केंद्रीय कार्यालय, 2री मंज़िल , सेंटर I, वर्ल्ड ट्रेड सेंटर, कफ परेड, मुंबई-400 005
Department of Non Banking Regulation, Central Office, 2nd Floor, Centre I, WTC, Cuffe Parade, Mumbai – 400 005
Tel No:22189131 Fax No:22163768 Email :helpdnbr@rbi.org.in

Table of Contents

5	Monitoring
IV	**Operation of deposit account with NBFCs and money mules**
V	**Inter-Governmental Agreement (IGA) with United States of America (US) under Foreign Accounts Tax Compliance Act (FATCA)- Registration**
VI	**Constitution of Special Investigating Team – sharing of information**

I. 'Know Your Customer' (KYC) Guidelines – Anti Money Laundering Standards

Introduction

The 'Know Your Customer' guidelines were issued in February 2005 revisiting the earlier guidelines issued in January 2004 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). These standards have become the international benchmark for framing Anti Money Laundering and combating financing of terrorism policies by the regulatory authorities. Compliance with these standards by the banks/financial institutions/NBFCs in the country have become necessary for international financial relationships. The Department of Banking Operations and Development of Reserve Bank had issued detailed guidelines to the banks 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, a copy of same is enclosed as per Annex-VI. These guidelines are equally applicable to NBFCs. All NBFCs were, therefore, advised to adopt the same with suitable modifications depending on the activity undertaken by them and ensure that a proper policy framework on 'Know Your Customer' and Anti-Money Laundering measures is formulated and put in place with the approval of the Board. NBFCs were advised to ensure that they are fully compliant with the instructions before December 31, 2005.

2. General Guidelines

While preparing operational guidelines, NBFCs were advised to bear in mind that the information collected from the customer for the purpose of opening of account should be kept as confidential and any details thereof should not be divulged for cross selling or any other purposes. NBFCs may, 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. Any other

information from the customer should be sought separately with his /her consent and after opening the account.

3. Definitions

3.1 Customer

For the purpose of KYC Norms, a ‘Customer’ is defined as a person who is engaged in a financial transaction or activity with 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 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 an 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. Further, it is clarified that NBFCs can also designate a person who holds the position of senior management or equivalent as a "Designated Director". In view of the above amendment, NBFCs were advised to nominate a Director on their

Boards as “designated Director” to ensure compliance with the obligations under the Prevention of Money Laundering (Amendment) Act, 2012.

However, in no case, the Principal Officer should be nominated as the "Designated Director".

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. Guidelines for NBFCs and persons authorised by NBFCs including brokers/agents etc.

As it is necessary that the guidelines should be equally applicable to the persons authorised by NBFCs including brokers/agents etc. collecting public deposits on behalf of NBFCs, it was advised on October 11, 2005 that:

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

As regards deposits collected by persons authorised by NBFCs including brokers/agents etc. in as much as such persons are collecting the deposits on behalf of the NBFC, it shall be the sole responsibility of the NBFC to ensure full compliance with the KYC guidelines by such persons. The NBFC should make available all information to the Bank to verify the compliance with the KYC guidelines and accept full consequences of any violation by the persons authorised by NBFCs including brokers/agents etc. who are operating on its behalf.

With regard to RNBCs a separate CC No.46 dated December 30, 2004 was issued delineating a road map for them wherein the guidelines were issued as under:

'In respect of new customers acquired after April 1, 2004, KYC guidelines as stated in the circular CC No.48 should be complied with in all cases. However, for the existing customers, initially, KYC guidelines should be complied in respect of large customers whose aggregate deposit exceeds Rs.1 lakh. For the remaining existing accounts, the companies should ensure that the details of the customers are updated at the time of renewal of the deposit. This should, however, not result in unnecessary harassment of customers.

As regards deposits collected by agents / sub-agents in as much as the agent / sub-agent is collecting the deposits on behalf of the RNBC, it shall be the sole responsibility of the RNBC to ensure full compliance with the KYC guidelines by its agents and sub-agents. The RNBC should make available all information to the regulator or his nominee to verify the compliance with the KYC guidelines and accept full consequences of any violation by the agent / sub-agent who is operating on its behalf.'

ii Due diligence of persons authorised by NBFCs including brokers/agents etc.

As an extension of the KYC Guidelines, NBFCs are required to put in place a process of due diligence in respect of persons authorised by NBFCs including brokers/agents etc. collecting deposits on behalf of the company through a uniform policy for appointment and detailed verification. Details of due diligence conducted may be kept on record with the company for verification.

In the depositors' interests and for enhancing transparency of operations, the companies should have systems in place to ensure that the books of accounts of persons authorised by NBFCs including brokers/agents etc, so far as they relate to brokerage functions of the company, are available for audit and inspection whenever required. RNBCs were also advised on the same lines vide CC No 46 dated December 30, 2004 mentioned above and were advised to report compliance to RBI by January 31, 2005.

iii. Customer service in terms of identifiable contact with persons authorised by NBFCs including brokers/agents etc.

All deposit receipts should bear the name and Registered Office address of the NBFC and must invariably indicate the name of the persons authorised by NBFCs including brokers/agents etc. and their addresses who mobilised the deposit and the link office with the telephone number of such officer and/or persons authorised by NBFCs including brokers/agents etc. in order that there is

a clear indication of the identifiable contact with the field persons and matters such as unclaimed / lapsed deposits, discontinued deposits, interest payments and other customer grievances are appropriately addressed. NBFCs should also have suitable review procedures to identify persons authorised by them including brokers/agents etc. in whose cases the incidence of discontinued deposits is high for taking suitable action.

RNBCs were also advised on the same lines vide CC No 46/02.02(RNBC)/2004-05 dated December 30, 2004.

5. In March, 2006, the KYC procedure was further simplified for opening accounts by NBFCs for those persons who intend to keep balances not exceeding rupees fifty thousand (Rs. 50,000/-) 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/-) in a year.

6. Accordingly, in case a person who wants to open an account is not able to produce documents mentioned in Annexure VIII to this circular, NBFCs may open accounts as described in paragraph 5 above, subject to

a) introduction from another account holder who has been subjected to full KYC procedure. The introducer's account with the NBFC should be at least six month old and should show satisfactory transactions. Photograph of the customer who proposes to open the account and also his address needs to be certified by the introducer.

or

b) any other evidence as to the identity and address of the customer to the satisfaction of the NBFC.

7. 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 NBFC (taken together) exceed rupees fifty thousand (Rs. 50,000/-) or total credit in the account exceeds rupees one lakh (Rs. 1, 00,000/-), no further transactions will be permitted until the full KYC procedure is completed. In order not to

inconvenience the customer, the NBFC must notify the customer when the balance reaches rupees forty thousand (Rs. 40,000/-) or the total credit in a year reaches rupees eighty thousand (Rs. 80,000/-) that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account will be stopped when the total balance in all the accounts taken together exceeds rupees fifty thousand (Rs. 50,000/-) or the total credit in the accounts exceeds rupees one lakh (Rs. 1,00,000/-) in a year. NBFCs were advised to issue suitable instructions to their branches for implementation in this regard.

8. In this regard, the term **'being satisfied'** as mentioned in Annex –VI means that the NBFC 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. An **indicative list** of the nature and type of documents/ information that may be relied upon for customer identification is given in the Annex-VIII to this circular. It may happen that Annex-VIII, which was clearly termed as an indicative list, may be treated by some NBFCs as an exhaustive list as a result of which a section of public may be denied access to financial services. NBFCs were, therefore, advised to take a review of their extant internal instructions in this regard.

9. In case of close relatives, e.g. husband, wife, son, daughter and parents, etc. who live with their wife, husband, father/mother, daughter and son, who do not have officially valid document for address verification, then, in such cases, banks/FIs should 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. NBFCs can use any supplementary evidence such as a letter received through post for further verification of the address. While issuing operational instructions to the branches on the subject, NBFCs should keep in mind the spirit of instructions issued by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.

10. It has been decided to simplify the requirement of submission of 'proof of address' as follows:

a) Customers may submit only one documentary proof of address (either current or permanent) while opening a deposit 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 NBFC 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 NBFC may take a declaration of the local address on which all correspondence will be made by the NBFC with the customer. No proof is required to be submitted for such address for correspondence/local address. This address may be verified by the NBFC through 'positive confirmation' such as acknowledgment of receipt of (i) letter (ii) telephonic conversation; (iii) visits; etc. In the event of change in this address due to relocation or any other reason, customers may intimate the new address for correspondence to the NBFC within two weeks of such a change.

11. Further, NBFCs, need not seek fresh proofs of identity and address at the time of periodic updation, from those customers who are categorised as 'low risk', in case of no change in status with respect to their identities and addresses. A self-certification by the customer to that effect should suffice in such cases. In case of change of address of such 'low risk' customers, they could merely forward a certified copy of the document (proof of address) by mail / post, etc. If an existing KYC compliant customer of NBFC desires to open another account in the same NBFC, there should be no need for submission of fresh proof of identity and / or proof of address for the purpose.

12. In terms of extant instructions, NBFCs are required to put in place a system of periodical review of risk categorisation of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Such review of risk categorisation of customers should be carried out at a periodicity of not **less** than once in six months. NBFCs were also advised to

introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. Accordingly, NBFCs are required to undertake 'Client Due Diligence' and apply such measures to existing clients based on risk categorization.

a) NBFCs would need to continue to carry out on-going due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and, wherever necessary, the source of funds.

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

c) Full KYC exercise will be required to be done at least every ten years for low risk and at least every eight years for medium risk individuals and entities taking in to account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained. Physical presence of the clients may, however, not be insisted upon at the time of such periodic updations.

d) Fresh photographs will be required to be obtained from minor customer on becoming major.

13. KYC/AML guidelines issued by the Bank shall also apply to NBFCs' branches and majority owned subsidiaries located outside India, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. In case, there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of NBFCs are required to adopt the more stringent regulation of the two.

14. Letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number

Subsequent to the Government of India Notification No. 14/2010/F.No. 6/2/2007-ES dated December 16, 2010, the letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number, can be accepted as an officially valid document as contained in Rule 2(1)(d) of the PML Rules, 2005. While opening accounts based on Aadhaar also, NBFCs must satisfy themselves about the current address of the customer by obtaining required proof of the same as per extant instructions.

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. Further, the information containing demographic details and photographs made available from UIDAI as a result of e-KYC process ("which is in an electronic form and accessible so as to be usable for a subsequent reference") 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 NBFC branches. The UIDAI then transfers the data of the individual comprising name, age, gender, and photograph of the individual, electronically to the NBFCs, which may be accepted as valid process for KYC verification. The broad operational instructions to NBFCs willing to use the UIDAI e-KYC service on Aadhaar e-KYC service are enclosed as Annex IX. Such NBFCs are advised to have proper infrastructure (as specified in Annex IX) in place to enable biometric authentication for e-KYC. Physical Aadhaar card / letter issued by UIDAI containing details of name, address and Aadhaar number received through post would continue to be accepted as an 'Officially Valid Document'.

Further, NBFCs may accept e-Aadhaar downloaded from UIDAI website as an officially valid document subject to the following:

a) If the prospective customer knows only his / her Aadhaar number, the NBFC may print the prospective customer's e-Aadhaar letter in the NBFC directly from the UIDAI portal; or adopt e-KYC procedure as mentioned above.

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

15. Allocation of Unique Customer Identification Code

In the context of recommendations of Working Group constituted by the Government of India regarding the introduction of unique identifiers for customers across different Financial Institutions for setting up a centralized KYC Registry, non-deposit taking NBFCs with asset size of Rs. 25 crore and above and all Deposit taking NBFCs have been advised to allot UCIC while entering into new relationships with individual customers as also the existing customers. A Unique Customer Identification Code (UCIC) will help NBFCs to identify the customers, avoid multiple identities, track the facilities availed, monitor financial transactions in a holistic manner and enable NBFCs to have a better approach to risk profiling of customers.

16. Accounts of Politically Exposed Persons (PEPs)

(1) Detailed guidelines on Customer Due Diligence (CDD) measures to be made applicable to Politically Exposed Person (PEP) and their family members or close relatives are contained in Annex VII. In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, NBFCs (including RNBCs) should obtain senior management approval to continue the business relationship and subject the account to the CDD measures as applicable

to the customers of PEP category including enhanced monitoring on an ongoing basis.

The instructions are also applicable to accounts where PEP is the ultimate beneficial owner. Further, in regard to PEP accounts, NBFCs should have appropriate ongoing risk management procedures for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which PEP is the ultimate beneficial owner.

17. Client accounts opened by professional intermediaries

When the NBFC 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. NBFCs may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. NBFCs also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the NBFCs 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 NBFC, the NBFC should still look through to the beneficial owners.

Further, in terms of paragraph 3 of Annex-VI, if an NBFC decides to accept an account in terms of the Customer Acceptance Policy, the NBFC should take reasonable measures 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. Therefore, under the extant AML/CFT framework, it is not possible for professional intermediaries like Lawyers and Chartered Accountants, etc. who are bound by any client confidentiality that prohibits disclosure of the client details, to hold an account on behalf of their clients.

Therefore, NBFCs should not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered

Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits NBFC's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, should not be allowed to open an account on behalf of a client.

18. Accounts of proprietary concerns

NBFCs have been advised that internal guidelines for customer identification procedure of legal entities may be framed by them based on their experience of dealing with such entities, normal lenders prudence and the legal requirements as per established practices. If the NBFCs/RNBCs decide to accept such accounts in terms of the Customer Acceptance Policy, the NBFC should take reasonable measures 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.

Further they were advised that for sake of clarity, in case of accounts of proprietorship concerns, to lay down criteria for the customer identification procedure for account opening by proprietary concerns. Accordingly, apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, NBFCs/RNBCs should call for and verify the following documents before opening of accounts in the name of a proprietary concern:

i) 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 & Establishment Act, sales and income tax returns, CST / VAT certificate, certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities, licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants

of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, etc.

ii) Any registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/ Department. NBFCs/RNBCs may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of account.

iii) 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.

iv) Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern.

v) Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.

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

19. Beneficial ownership

When an NBFC identifies a customer for opening an account, it should 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.

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

20. Principal Officer

NBFCs (including RNBCs) have been advised in Para 4(x) of Annex VI that they should appoint a senior management officer to be designated as Principal Officer and the role and responsibilities of the Principal Officer have been detailed therein. With a view to enable the Principal Officer to discharge his responsibilities, 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, NBFCs (including RNBCs) should ensure that the Principal Officer is able to act independently and report directly to the senior management or to the Board of Directors. The role and responsibilities of the Principal Officer should include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made thereunder, as amended form time to time.

21. Suspicion of money laundering/terrorist financing

With a view to preventing NBFCs from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing, whenever there is suspicion of money laundering or terrorist financing or when other factors give rise to a belief that the customer does not, in fact, pose a low risk, NBFCs shall carry out full scale customer due diligence (CDD) before opening an account.

22. Filing of Suspicious Transaction Report (STR)

In terms of Para 3.2.2 of Annex-VI, an NBFC should not open an account (or should consider closing an existing account) when it is unable to apply appropriate CDD measures. In the circumstances, when an NBFC believes that it would no longer be satisfied that it knows the true identity of the account holder, the Company should also file an STR with FIU-IND.

II. Prevention of Money Laundering Act, 2002 - Obligations of NBFCs in terms of Rules notified thereunder

1. NBFCs were advised to appoint a Principal Officer and put in place a system of internal reporting of suspicious transactions and cash transactions of Rs.10 lakh and above. In this connection, Government of India, Ministry of Finance, Department of Revenue, issued a notification dated July 1, 2005 in the Gazette of India, notifying the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts certain obligations on the NBFCs in regard to preservation and reporting of customer account information.

With the enactment of Prevention of Money Laundering (Amendment) Act, 2012 and amendment to Section 13 of the Act which provides for "Powers of Director to impose fine", the section 13(2) now reads as under:

"If the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may—

(a) issue a warning in writing; or

(b) direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or

(c) direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or

(d) by an order, levy a fine on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure."

2. Maintenance of records of transactions

2.1 NBFCs should introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005), 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 have taken place within a month and the monthly aggregate which exceeds rupees ten lakhs or its equivalent in foreign currency. It is clarified that for determining 'integrally connected transactions' 'all accounts of the same customer' should be taken into account.

(iii) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place facilitating the transactions;

(iv) all suspicious transactions whether or not made in cash and in manner as mentioned in the Rules framed by Government of India under the Prevention of Money Laundering Act, 2002.

NBFCs are required to adhere to the reporting requirements as per the amended rules.

2.2 NBFCs are required to 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.

3. Preservation of records

NBFCs should take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities

(i) In terms of PML Amendment Act 2012, NBFCs should maintain for at least five years from the date of transaction between the NBFC 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) NBFCs should ensure that 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, are properly preserved for at least five years after the business relationship is ended as required under Rule 10 of the Rules ibid. The identification of records and transaction data should be made available to the competent authorities upon request.

(iii) NBFCs may 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) As mentioned in para 3.3 of Annex VI, NBFCs are required 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 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.

4. Reliance on third party due diligence

For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, NBFCs may rely on a third party subject to the conditions that-

1) the NBFC immediately obtains necessary information of such client due diligence carried out by the third party;
2) the NBFC 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 NBFC 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 NBFC is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable

5. Reporting to Financial Intelligence Unit-India

5.1 In terms of the PMLA rules, NBFCs are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri,
New Delhi-110021

(i) There are altogether five reporting formats prescribed for a banking company viz. i) Manual reporting of cash transactions ii) Manual reporting of suspicious transactions iii) Consolidated reporting of cash transactions by Principal Officer of the bank iv) Electronic data structure for cash transaction reporting and v) Electronic data structure for suspicious transaction reporting which are enclosed to this circular. The reporting formats contain detailed guidelines on the compilation and manner/procedure of submission of the reports to FIU-IND. NBFCs were advised to adopt the format prescribed for banks with suitable modifications. NBFCs were also advised to initiate urgent steps to ensure electronic filing of cash transaction report (CTR) as early as possible. The related hardware and technical requirement for preparing reports in an electronic format, the related data files and data structures thereof were furnished in the instructions part of the concerned formats. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, NBFCs should scrupulously adhere to the following:

(a) The cash transaction report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month. While filing CTR, individual transactions below rupees fifty thousand may not be included. Cash transaction reporting by branches/offices of NBFCs to their Principal Officer should invariably be submitted on monthly basis (not on fortnightly basis) and the Principal Officer, in turn, should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule;

(b) 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;

(c) The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND;

(d) Utmost confidentiality should be maintained in filing of CTR and STR with FIU-IND. The reports may be transmitted by speed/ registered post, fax, email at the notified address;

(e) It should be ensured that the reports for all the branches are filed in one mode i.e. electronic or manual;

(f) A summary of cash transaction report for the NBFC as a whole may be compiled by the Principal Officer of the NBFC in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted both for manual and electronic reporting.

5.2. In paragraph 7 of our circular dated April 5, 2006, NBFCs were advised to initiate urgent steps to ensure electronic filing of cash transaction report (CTR) and Suspicious Transaction Reports (STR) to FIU-IND. In case of NBFCs, where all the branches are not yet fully computerized, the Principal Officer of the NBFC should cull out the transaction details from branches which are not computerized and suitably arrange to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on their website http://fiuindia.gov.in.

5.3. NBFCs may not put any restrictions on operations in the accounts where an STR has been made. However, it should be ensured that there is no tipping off to the customer at any level. It is likely that in some cases, transactions are abandoned/ aborted by customers on being asked to give some details or to provide documents. NBFCs should report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

5.4. In regard to CTR, the cut-off limit of Rupees ten lakh is applicable to integrally connected cash transactions also. Further, after consultation with FIU-IND, it is clarified that:

a) For determining integrally connected cash transactions, NBFCs should take into account all individual cash transactions in an account during a calendar month, where either debit or credit summation, computed separately, exceeds Rupees ten lakh during the month. However, while filing CTR, details of individual cash transactions below rupees fifty thousand may not be indicated. Illustration of integrally connected cash transactions is furnished in Annex-I;

b) CTR should contain only the transactions carried out by the NBFC on behalf of their clients/customers excluding transactions between the internal accounts of the NBFC;

c) 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 format (Counterfeit Currency Report – CCR) as per Annex-II. Electronic data structure has been furnished in Annex-IV to enable NBFCs to generate electronic CCRs. 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.

The multiple data files reporting format were replaced by a new single XML file format as provided in the 'Download' section of the FIU-IND website (http://fiuindia.gov.in/). All NBFCs were requested to carefully go through the revised reporting format and initiate urgent steps to build capacity to generate reports, which are compliant with the new reporting XML format specifications.

FIU-IND had advised vide their letter F.No.9-29/2011-FIU-IND dated August 28, 2012, that all NBFCs should initiate submission of reports on the FINnet Gateway in 'TEST MODE' from August 31, 2012 to test their ability to upload the report electronically. Such submission in 'Test Mode' was to be continued till FIU-IND informs the NBFCs about 'go-live' of the project.

As the project has gone 'live' NBFCs were advised to discontinue submission of reports in CD, using only FINnet gateway for uploading of reports in the new XML

reporting format. Any report in CD will not be treated as a valid submission by FIU-IND. For any clarification / assistance regarding submission of reports, NBFCs may contact FIU-IND help desk at email or telephone numbers 011-24109792/93.

5.5 While making STRs, NBFCs should be guided by the definition of 'suspicious transaction' as contained in Rule 2(g) of Rules ibid. NBFCs should make STRs if they have 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.

5.6 In terms of Rule 8, while furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall constitute a separate violation. Banks/FIs are advised to take note of the timeliness of the reporting requirements.

6. In terms of instructions contained in the guidelines on ‘Know Your Customer Norms’ and ‘Anti-Money Laundering Measures’ of our circular dated February 21, 2005, NBFCs are required to prepare a profile for each customer based on risk categorization. Further, vide paragraph 4 of our circular DNBS (PD). CC 68 /03.10.042/2005-06 dated April 5, 2006, the need for periodical review of risk categorization has been emphasized. NBFCs, as a part of transaction monitoring mechanism, were 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 transactions.

7. As stated in para 3.3 of Annex VI, NBFCs are required 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. 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. These records are required to be preserved for ten years as is required under PMLA, 2002. Such records and related documents should be made available to help auditors in their work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities.

8. 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) Amendment Rules, 2009/10 - Obligation of banks/Financial institutions

Government of India vide its Notifications No.13/2009/F.No.6/8/2009-ES dated November 12, 2009, February 12, 2010 and June 16, 2010 amended 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. NBFCs and RNBCs were advised to study details of notification and the amendments clearly noted and spread across their organisation and to strictly follow the amended provisions of PMLA Rules and ensure meticulous compliance with these Rules.

9. Assessment and Monitoring of Risk

The Government of India had constituted a National Money Laundering/Financing of Terror Risk Assessment Committee to assess money laundering and terror

financing risks, a national AML/CFT strategy and institutional framework for AML/CFT in India. Assessment of risk of Money Laundering /Financing of Terrorism helps both the competent authorities and the regulated entities in taking necessary steps for combating ML/FT adopting a risk-based approach. This helps in judicious and efficient allocation of resources and makes the AML/CFT regime more robust. The Committee made recommendations regarding adoption of a risk-based approach, assessment of risk and putting in place a system which would use that assessment to take steps to effectively counter ML/FT. The recommendations of the Committee were accepted by the Government of India for implementation.

Accordingly, NBFCs were advised to take steps to identify and assess their ML/FT risk for customers, countries and geographical areas as also for products/ services/ transactions/delivery channels, in addition to what has been prescribed in Annex VI para 3.4. NBFCs should have policies, controls and procedures, duly approved by their boards, in place to effectively manage and mitigate their risk, adopting a risk-based approach as discussed above. As a corollary, NBFCs would be required to adopt enhanced measures for products, services and customers with a medium or high risk rating.

In this regard, Indian Banks' Association (IBA) had taken initiative in assessment of ML/FT risk in the banking sector. This has been circulated to its member banks on May 18, 2011 and a copy of their Report on Parameters for Risk Based Transaction Monitoring (RBTM) as a supplement to their guidance note on Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards issued in July 2009, is available on the IBA website. The IBA guidance also provides an indicative list of high risk customers, products, services and geographies. NBFCs were advised to use the same as guidance in their own risk assessment.

In order to have an effective implementation of KYC/AML/CFT measures, NBFCs were advised to put in place a system of periodic review of risk categorization of

customers and updation of customer identification data in a time-bound manner, and in any case not later than end-March 2013.

III. Combating financing of terrorism

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. NBFCs were, therefore, advised to develop suitable mechanism through appropriate policy framework for 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.

1. As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank circulates these to all banks and financial institutions (including NBFCs). NBFCs should ensure to update the consolidated list of individuals and entities as circulated by Reserve Bank. Further, the updated list of such individuals/entities can be accessed in the United Nations website at http://www.un.org/sc/committees/1267/consolist.shtml. NBFCs are advised that before opening any new account, it should be ensured that the name/s of the proposed customer does not appear in the list. Further, NBFCs should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to RBI and FIU-IND.

2. 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/financial channels. It would, therefore, be necessary that adequate

screening mechanism is put in place by NBFCs as an integral part of their recruitment/hiring process of personnel.

3. In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, NBFCs may consider the indicative list of suspicious activities contained in Annex-V.

4. Countries which do not or insufficiently apply the FATF recommendations

Financial Action Task Force (FATF) has issued several Statements on risks arising from the deficiencies in AML/CFT regime of various countries for example Uzbekistan, Iran, Pakistan, Turkmenistan, Sao Tome and Principe on etc. which are updated from time to time. All NBFCs/RNBCs were required to consider the information contained in the statements issued by FATF which however, does not preclude financial institutions from legitimate trade and business transactions with the countries and jurisdictions mentioned in the statement.

NBFCs should take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement. NBFCs should, in addition to FATF Statements circulated by Reserve Bank from time to time, also consider publicly available information for identifying such countries, which do not or insufficiently apply the FATF Recommendations. NBFCs should give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in these countries.

5. Monitoring

In terms of para 3.3 of Annex-VI, ongoing monitoring is an essential element of effective KYC procedures. It is advised that NBFCs should 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 be retained and made available to Reserve Bank/other relevant authorities, on request.

NBFCs should apply enhanced due diligence measures on high risk customers. Some illustrative examples of customers requiring higher due diligence are given in the paragraph under reference. In view of the risks involved in cash intensive businesses, accounts of bullion dealers(including sub-dealers) and jewelers should also be categorized by NBFCs as 'high risk' requiring enhanced due diligence.

Ongoing monitoring is an essential element of effective KYC procedures. NBFCs are also required to subject these 'high risk accounts' to intensified transaction monitoring. High risk associated with such accounts should be taken into account by NBFCs to identify suspicious transactions for filing Suspicious Transaction Reports (STRs) to FIU-ND.

IV. Operation of deposit account with NBFCs and money mules

It was brought to the notice of NBFCs /RNBCs that "Money mules" can be used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "money mules." In some cases, these third parties may be innocent while in others, they may be having complicity with the criminals.

NBFCS were advised to strictly adhere to the guidelines on KYC/AML/CFT issued from time to time and to those relating to periodical updation of customer identification data after the account is opened and also to monitoring of transactions in order to protect themselves and their customers from misuse by such fraudsters.

NBFCs were also advised to ensure that their accounts in banks are not used for the purpose of money laundering in the manner specified above.

These guidelines are issued under Sections 45K and 45L of the RBI Act, 1934 and any contravention of the same or non-compliance will attract penalties under the relevant provisions of the Act and Rule 7 of 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.

V. Inter-Governmental Agreement (IGA) with United States of America (US) under Foreign Accounts Tax Compliance Act (FATCA) - Registration

Government of India has now advised that to avoid withholding tax, Foreign Financial Institutions (FFIs) in Model 1 jurisdictions, such as India, need to register with IRS and obtain a Global Intermediary Identification Number (GIIN) before January 1, 2015. The FFIs who have registered but have not obtained a GIIN should indicate to the withholding agents that the GIIN is applied for, which may be verified by the withholding agents in 90 days. In this regard, the FAQ published on the IRS website (updated as on December 22, 2014), as received from the Government of India, is furnished in the circular DNBR.CC.PD.No.010/03.10.01/2014-15, dated January 9, 2015. Accordingly, NBFCs may take action appropriately.

VI. Constitution of Special Investigating Team – sharing of information

In pursuance of the Hon'ble Supreme Court Judgment dated July 4, 2011, Government of India has constituted a Special Investigation Team (SIT) under the Chairmanship of Hon'ble Justice M.B. Shah. In this regard, the Hon'ble Supreme Court had directed that:

"All organs agencies, departments and agents of the State, whether at the level of the Union of India, or the State Government, including but not limited to all statutorily formed individual bodies, and other constitutional bodies extend all the cooperation necessary for the functioning of the Special Investigation Team.

The Union of India and where needed the State Government will facilitate the conduct of the investigations, in their fullest measures, by the Special Investigation Team and functioning, by extending all necessary financial, material, legal, diplomatic and intelligence resources, whether such investigations or portions of such investigations occur inside the country or abroad."

In view of above, all NBFCs are advised to ensure that information/documents required by the SIT are made available as and when required.

-------*----------

Annex-I

Illustration of Integrally connected cash transaction

The following transactions have taken place in an NBFC during the month of April, 2008:

Date	**Mode**	**Dr. (in Rs.)**	**Cr. (in Rs.)**	**Balance (in 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	1,00,000.00	3,90,000.00
Monthly summation		10,10,000.00	6,00,000.00	

i) 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 lakhs. However, the NBFC should report only the debit transaction taken place on 02/04 & 08/04/2008. The debit transaction dated 07/04/2008 should not be separately reported by the NBFC, which is less than Rs.50, 000/-.

ii) 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 NBFC.

xxx

ANNEX - II

FIU-IND | Financial Intelligence Unit- India

COUNTERFEIT CURRENCY REPORT (CCR)

Kindly fill in CAPITAL. Read the instructions before filling the form.

PART 1 DETAILS OF REPORTING BRANCH/LOCATION

1.1	Name of Entity		
1.2	Name of Branch		
1.3	Branch Reference Number	1.4 ID allotted by FIU-IND	
1.5	Address *(No., Building)*		
1.6	Street/Road		
1.7	Locality		
1.8	City/Town, District		
1.9	State, Country		
1.10	Pin code	1.11 Tel *(with STD code)*	
1.12	Fax	1.13 E-mail	

PART 2 DETAILS OF COUNTERFEIT CURRENCY

	Denomination	Number of pieces	Value
2.1	1000		
2.2			
2.3			
2.4			
2.5	20		
2.6	10		
2.7			
	2.8 **Total Value of Counterfeit Currency**		

PART 3 DETAILS OF DETECTION

3.1 Date of Cash Tendering

3.2 Total Cash Deposited

3.3 Date of Detection

3.4 Detected at

- A Cash Counter
- B Branch Level
- C Currency Chest
- D RBI's CVPS
- Z Other

3.5 Whether local police station has been informed — Yes / No

3.6 Details of FIR *(if available)*

3.7 Additional Information, if any

PART 4 DETAILS OF RELATED PERSONS

4.1 Name of Tendering Person

4.2 Name of Account Holder

4.3 Account / Card No.

Signature

Name

Designation

DO NOT FILL. FOR FIU-IND USE ONLY. | CCR

COUNTERFEIT CURRENCY REPORT (CCR)

INSTRUCTIONS

GENERAL INSTRUCTIONS

Under the Prevention of Money Laundering Act 2002 (PMLA), every reporting entity is required to furnish details of all cash transactions where forged or counterfeit currency notes of bank notes have been used as genuine. These transactions should be reported to Director, Financial Intelligence Unit, India not later than seven working days from the date of occurrence of such transactions.

HOW TO SUBMIT

Every reporting entity branch must submit this form to the Director, FIU- IND only through the principal officer designated under PMLA.

Note: A separate Counterfeit Currency Report (CCR) should be filed for each incident of detection of counterfeit Indian currency. If the detected counterfeit currency notes can be segregated on the basis of tendering person, a separate CCR should be filed for each such incident.

EXPLANATION OF SPECIFIC TERMS

PART 1: DETAILS OF REPORTING BRANCH / LOCATION

This section contains details of the branch/location where the counterfeit currency was detected.

1.1 Mention name of the reporting entity (bank, financial institution).

1.2 Mention name of the reporting branch/location.

1.3 Mention any unique number issued by the regulator or any temporary code to uniquely identify each branch/ location.

1.4 ID allotted by FIU-IND may be left blank till the same is communicated by FIU-IND.

1.10 Pincode should be a valid 6 digit numeric pincode of the branch/location.

PART 2: DETAILS OF COUNTERFEIT CURRENCY

This section contains the details of counterfiet currency. Total value of counterfeit currency should match with the total calculated value of Denomination x Number of pieces.

PART 3: DETAILS OF DETECTION

3.1 Mention the date on which cash was tendered, if available. Date should be reported in YYYYMMDD format. E.g. 2nd May, 2007 should be entered as 20070502.

3.2 Mention the total cash tendered by the renderer including counterfeit currency, if available.

3.3 Mention the date on which counterfeit currency was detected in YYYYMMDD format. E.g. 2nd May 2007 should be entered as 20070502.

3.4 Select from the following counterfeit currrency detection stages

"A"- Cash Counter by the teller
"B"- Branch Level during sorting
"C"- Currency Chest while counting
"D"- Currency Verification and Processing System at RBI
"Z"- Other

3.5 Mention Yes, if local police station has been informed.

3.6 Mention details of FIR, polic station etc., if available.

3.7 Mention addtional information such as quality of counterfeit currency, sequence of events, if available.

PART 4: DETAILS OF RELATED PERSONS

4.1 Person who tendered the counterfeit currency, if available.

4.2 Name of the sole/first account holder in whose account counterfiet currency was tendered, if available.

4.3 Account/Card Number of the person in whose account the counterfeit currency was tendered, if available.

The form should be signed by an officer at the branch/controlling office/head office.

ANNEX - III

FIU-IND

Financial Intelligence Unit- India

SUMMARY OF COUNTERFEIT CURRENCY REPORTS

Kindly fill in CAPITAL. Read the instructions before filling the form.

PART 1 DETAILS OF THE PRINCIPAL OFFICER

1.1	Name of Reporting Entity		
1.2	Branch Reference Number	1.3 ID allotted by FIU-IND	
1.4	Category of Entity	*(Refer to Instructions)*	
1.5	Name of Principal Officer		
1.6	Designation		
1.7	Address *(No., Building)*		
1.8	Street/Road		
1.9	Locality		
1.10	City/Town, District		
1.11	State, Country		
1.12	Pin code	1.13 Tel *(with STD code)*	
1.14	Fax	1.15 E-mail	

PART 2 STATISTICS

2.1	Number of Counterfeit Currency Reports enclosed	
2.2	Total Value of Counterfeit Currency	

DO NOT FILL. FOR FIU-IND USE ONLY

ACK. NO.

DATE 2 0 0 (D D M M Y Y Y Y)

Signature

Name

(Should be same as the person mentioned in PART 1)

Date

DO NOT FILL. FOR FIU-IND USE ONLY. CCRS

SUMMARY OF COUNTERFEIT CURRENCY REPORTS (CCRs)

INSTRUCTIONS

GENERAL INSTRUCTIONS

Under the Prevention of Money Laundering Act 2002 (PMLA), every reporting entity (bank, financial instituion, intermediary) is required to furnish details of all cash transactions where forged or counterfeit currency notes of bank notes have been used as genuine. These transactions should be reported to Director, Financial Intelligence Unit, India not later than seven working days from the date of occurrence of such transactions.

One CCR should be submitted for each incident of detection of counterfeit Indian currency. If the counterfeit currency detected can be segregated on the basis of tendering person, a separate CCR should be filed for each such incident.

How to submit

The principal officer should submit this summary alongwith CCRs received from branches /locations to the Director, FIU-IND.

Address Director, FIU-IND
Financial Intelligence Unit-India
6th Floor, Hotel Samrat
Chanakyapuri, New Delhi -110021
India

EXPLANATION OF SPECIFIC TERMS

PART 1: DETAILS OF THE PRINCIPAL OFFICER

1.3. ID allotted by FIU-IND may be left blank till the same is communicated by FIU-IND.

1.4. Category of the reporting entity

"A"-Public Sector Bank
"B"-Private Sector Bank
"C"-Foreign Bank
"D"-Co-operative Bank
"E"-Regional Rural Bank
"F"-Local Area Bank
"Z"-Other

1.5. Principal officer is the officer designated under PMLA.

PART 2: STATISTICS

2.1. Number of Counterfeit Currency Reports enclosed.

2.2. Total Value of counterfeit currency detected in the enclosed reports. (Sum of value is in 2.8 of each CCR).

ALL CCRs MUST BE ENCLOSED.

ANNEX - IV

ELECTRONIC DATA STRUCTURE

Report	COUNTERFEIT CURRENCY REPORT
Version	1.0

Contents

Appendix

Counterfeit Currency Report
Summary of Counterfeit Currency Report

1. Introduction

The Prevention of Money Laundering Act, 2002 (PMLA) forms the core of the legal framework put in place by India to combat money laundering. PMLA and the Rules notified thereunder came into force with effect from July 1, 2005. Director, FIU-IND and Director (Enforcement) have been conferred with exclusive and concurrent powers under relevant Sections of the Act to implement the provisions of the Act.

2. Counterfeit Currency Report

The PMLA and Rules notified thereunder impose an obligation on banks, financial institutions and intermediaries of the securities market (reporting entity) to furnish details of all cash transactions where forged or counterfeit currency notes of bank notes have been used as genuine to the Director, FIU-IND.

A separate Counterfeit Currency Report (CCR) should be filed for each incident of detection of counterfeit Indian currency. If the detected counterfeit currency notes can be segregated on the basis of tendering person, a separate CCR should be filed for each such incident.

3. Due Date

These transactions should be reported to Director, Financial Intelligence Unit, India not later than seven working days from the date of occurrence of such transactions.

4. Methods of filing

The CCR should be submitted to the Financial Intelligence Unit – India (FIU-IND) at the following address:

Director, FIU-IND
Financial Intelligence Unit-India
6th Floor, Hotel Samrat
Chanakyapuri, New Delhi -110021, India
(Visit http://fiuindia.gov.in for more details)

Counterfeit Currency Reports can be filed either in manual or electronic format. However, the reporting entity must submit all reports to FIU-IND in electronic format if it has the technical capability to do so.

For reporting entities, which do not have technical capacity to generate report in electronic form, a report preparation utility for preparation of electronic Counterfeit Currency Report (CCRRPU.xls) can be downloaded from the website of the FIU-IND at http://fiuindia.gov.in

5. Manual format

Counterfeit Currency Reports in manual format consists of following forms:

Form	Information	Completed by
Summary of Counterfeit Currency Reports	Contains summary of enclosed CCRs	Principal officer of the reporting entity
Counterfeit Currency Report	Details of branch and counterfeit currency.	Reporting branch/office

The above forms are given in the Appendix.

6. Electronic format

FIU-IND is in the process of developing technological infrastructure to enable submission of electronic return over a secure gateway. In the interim, the reporting entities should submit the following to Director, FIU-IND:

i) One CD containing three data files in prescribed data structure. A label mentioning name of the reporting entity, Unique code, type of report (CCR), report dated should be affixed on each CD for the purpose of identification.

ii) Each CD should be accompanied by Summary of Counterfeit Currency Report for Reporting entity (same form should be used for both manual as well as electronic format) in physical form duly signed by the principal officer. This summary should match with the data in Control File (CCRCTL.txt).

Important:

i) In case the size of data files exceeds the capacity of one CD, the data files should be compressed by using Winzip 8.1 or ZipItFast 3.0 (or higher version) compression utility only to ensure quick and smooth acceptance of the file.

ii) The CD should be virus free.

7. Description of Data Files

In case of electronic filing, the consolidated CCR data should have following three data files:

S No.	Filename	Description
1	CCRCTL.txt	Control File
2	CCRBRC.txt	Branch File
3	CCRTRN.txt	Transaction File

8. Steps in preparation of data files

i) The details of counterfeit currency should be captured in the Transaction File (CCRTRN.txt).

ii) The details of branches should be captured in the Branch File (CCRBRC.txt).

iii) The report level details and summary should be captured in the Control file. (CCRCTL.txt)

9. Steps in validation /sufficiency of data files

i) There should be three data files with appropriate naming convention.

ii) The data files should be as per specified data structure and business rules.

iii) None of the mandatory fields should be left blank.

iv) All dates should be entered in YYYYMMDD format.

v) The summary figures in control file should match with the totals in other data files.

vi) [Branch Reference Number] should be unique in Branch Data File (CCRBRC.txt)

vii) All values of [Branch Reference Number] in Transaction Data File (CCRTRN.txt) should have matching [Branch Reference Number] value in Branch Data File (CCRBRC.txt)

10. General notes for all Data Files

i) All Data Files should be generated in ASCII Format with ".txt" as filename extension.

ii) Each Record (including last record) must start on new line and must end with a newline character. Hex Values: "0D" & "0A".

iii) All CHAR fields must be left justified.

iv) If CHAR field has no data or less data with respect to defined length, then the entire field (in case of no data) or the remaining field (in case of less data) has to be filled with right justified blank characters (Spaces).

v) All NUM fields must be right justified.

vi) If NUM field has no data or less data with respect to defined length, then the entire field (in case of no data) or the remaining field (in case of less data) has to be filled with left justified zeroes.

vii) If DATE field has no data then the entire field has to be filled with blank characters (Spaces).

viii) Fields with an asterisk (*) have to be compulsorily filled up.

ix) For fields that do not have an asterisk (*), reasonable efforts have to be made to get the information. Enter "N/A" to indicate that the field is not applicable. Do not substitute any other abbreviations or special characters (e.g., "x", "-" or "*").

11. Data structure of Control File (CCRCTL.txt)

S. No.	Field	Type	Size	From	To	Remarks
1.	Report Name*	CHAR	3	1	3	Value should be "CCR" signifying Counterfeit Currency Report
2.	Serial Number of Report*	NUM	8	4	11	Indicates the running sequence number of CCR for the reporting entity starting from 1
3.	Record Type*	CHAR	3	12	14	Value should be "CTL" signifying Control file
4.	Report Date*	NUM	8	15	22	Date of sending report to FIU-IND in YYYYMMDD format
5.	Reporting Entity Name*	CHAR	80	23	102	Complete name of the reporting entity (Bank, financial institution, intermediary)
6.	Reporting Entity Category*	CHAR	1	103	103	"A"-Public Sector Bank "B"-Private Sector Bank "C"-Foreign Bank "D"-Co-operative Bank "E"-Regional Rural Bank "F"-Local Area Bank "Z"-Other
7.	Unique code of the Reporting Entity*	CHAR	12	104	115	Unique code issued by the regulator, if applicable
8.	Unique ID issued by FIU*	CHAR	10	116	125	Use XXXXXXXXXX till the ID is communicated
9.	Principal Officer's Name*	CHAR	80	126	205	Field + filler spaces = 80
10.	Principal Officer's Designation*	CHAR	80	206	285	Field + filler spaces = 80
11.	Principal Officer's Address1*	CHAR	45	286	330	No., Building Field + filler spaces = 45
12.	Principal Officer's Address2	CHAR	45	331	375	Street/Road Field + filler spaces = 45
13.	Principal Officer's Address3	CHAR	45	376	420	Locality Field + filler spaces = 45
14.	Principal Officer's Address4	CHAR	45	421	465	City/Town, District Field + filler spaces = 45
15.	Principal Officer's Address5	CHAR	45	466	510	State, Country Field + filler spaces = 45

16.	Principal Officer's Pin code*	NUM	6	511	516	Pin code without "-" or space
17.	Principal Officer's Telephone	CHAR	30	517	546	Telephone in format STD Code-Telephone number
18.	Principal Officer's FAX	CHAR	30	547	576	Fax number in format STD Code-Telephone number
19.	Principal Officer's E-mail	CHAR	50	577	626	E-mail address
20.	Report Type*	CHAR	1	627	627	"N"- New Report "R"- Replacement to earlier submitted report
21.	Reason for Replacement*	CHAR	1	628	628	"A" – Acknowledgement of Original Report had many warnings or error messages. "B" – Operational error, data omitted in Original Report. "C" – Operational error, wrong data submitted in Original Report. "N"- Not Applicable as this is a new report "Z"- Other Reason
22.	Serial Number of Original Report *	NUM	8	629	636	Serial Number of the Original Report which is being replaced. Mention 0 if Report Type is "N"
23.	Operational Mode*	CHAR	1	637	637	"P"- Actual/ Production mode "T"- Test / Trial mode
24.	Data Structure Version*	CHAR	1	638	638	Value should be 1 to indicate Version 1.0
25.	Number of Counterfeit Currency Reports*	NUM	8	639	646	Number of CCRs enclosed in this summary. This figure should match with the number of records in CCRTRN.txt
26.	Total Value of Counterfeit Currency*	NUM	12	647	658	Total Value of Counterfeit Currency reported in enclosed CCRs. This figure should match with the sum of the Field Total Counterfeit Currency (S. No. 11) in CCRTRN.txt

12. Data structure of Branch File (CCRBRC.txt)

S. No.	Field	Type	Size	From	To	Remarks
1.	Record Type	CHAR	3	1	3	Value should be "BRC" signifying Control file
2.	Line Number*	NUM	6	4	9	Running Sequence Number for each line in the file starting from 1. This Number will be used during validation checks.
3.	Name of Branch*	CHAR	80	10	89	Name of branch/location where the counterfeit currency was tendered Field + filler spaces = 80
4.	Branch Reference Number*	CHAR	12	90	101	Unique Code issued by the regulator or any temporary code to uniquely identify each branch/office
5.	Unique ID issued by FIU*	CHAR	10	102	111	Use XXXXXXXXXX till the ID is communicated
6.	Branch Address1*	CHAR	45	112	156	No., Building Field + filler spaces = 45
7.	Branch Address2*	CHAR	45	157	201	Street/Road Field + filler spaces = 45
8.	Branch Address3	CHAR	45	202	246	Locality Field + filler spaces = 45
9.	Branch Address4	CHAR	45	247	291	City/Town, District Field + filler spaces = 45
10.	Branch Address5	CHAR	45	292	336	State, Country Field + filler spaces = 45
11.	Branch Pin code*	NUM	6	337	342	Pin code without "-" or space
12.	Branch Telephone	CHAR	30	343	372	Telephone number in format STD Code-Telephone number
13.	Branch Fax	CHAR	30	373	402	Fax number in format STD Code-Telephone number
14.	Branch E-mail	CHAR	50	403	452	E-mail address

13. Data structure of Transaction File (CCRTRN.txt)

S. No.	Field	Type	Size	From	To	Remarks
1.	Record Type*	CHAR	3	1	3	Value should be "TRN" signifying Transaction data file
2.	Line Number*	NUM	6	4	9	Running Sequence Number for each line in the file starting from 1. This Number will be used during validation checks.
3.	Branch Reference Number*	CHAR	12	10	21	Branch Reference Number of branch/location where counterfeit currency was tendered. Use any unique number issued by the regulator or any temporary code to uniquely identify each branch/ location
4.	Denomination1000	NUM	10	22	31	Number of counterfeit currency notes of Rs. 1000/- each
5.	Denomination500	NUM	10	32	41	Number of counterfeit currency notes of Rs. 500/- each
6.	Denomination100	NUM	10	42	51	Number of counterfeit currency notes of Rs. 100/- each
7.	Denomination50	NUM	10	52	61	Number of counterfeit currency notes of Rs. 50/- each
8.	Denomination20	NUM	10	62	71	Number of counterfeit currency notes of Rs. 20/- each
9.	Denomination10	NUM	10	72	81	Number of counterfeit currency notes of Rs. 10/- each
10.	Denomination5	NUM	10	82	91	Number of counterfeit currency notes of Rs. 5/- each
11.	Total Counterfeit Currency	NUM	10	92	101	Value of counterfeit currency detected. This value should match with the value derived from the number of notes mentioned in S. No. 4 to 10 above.
12.	Tendering Date	NUM	8	102	109	Date of tendering counterfeit currency in YYYYMMDD format, if available. E.g.: 2nd May 2007 should be written as 20070502
13.	Total Cash Tendered	NUM	20	110	129	Total Cash tendered by the tenderer including the counterfeit currency, if available
14.	Detection Date*	NUM	8	130	137	In YYYYMMDD format E.g.: 2nd May 2007 should be written as 20070502
15.	Detected At*	CHAR	1	138	138	"A"- Cash Counter "B"- Branch Level "C"- Currency Chest "D"- RBI's CVPS "Z"- Other

16.	Police Informed	CHAR	1	139	139	Y – for Yes, N – for No
17.	FIR Detail	CHAR	80	140	219	FIR, Police Station details etc., if available
18.	Additional Information	CHAR	80	220	299	Additional Information such as quality of counterfeit currency, sequence of events, if available
19.	Name of Tendering Person	CHAR	80	300	379	Person who tendered the counterfeit currency, if available.
20.	Name of Account Holder	CHAR	80	380	459	Name of the Sole/First account holder in whose account the counterfeit currency was tendered, if available.
21.	Account Number	CHAR	20	460	479	Account/Card Number of the person in whose account the counterfeit currency was tendered, if available.

Annex -V

An Indicative List of Suspicious Activities Transactions Involving Large Amounts of Cash

Company transactions, that are denominated by unusually large amounts of cash, rather than normally associated with the normal commercial operations of the company, e.g. cheques,

Transactions that do not make Economic Sense

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

Activities not consistent with the Customer's Business

Accounts with large volume of credits whereas the nature of business does not justify such credits.

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 NBFC employee not to file any reports or any other forms.

(iii) An account where there are several cash transactions 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.

Unusual Activities

Funds coming from the countries/centers which are known for money laundering.

Customer who provides Insufficient or Suspicious Information

(i) A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior business 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.

Certain NBFC 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.

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

- Large Cash Transactions
- Multiple accounts under the same name
- Placing funds in term Deposits and using them as security for more loans
- Sudden surge in activity level
- Same funds being moved repeatedly among several accounts

xxx

Annex-VI

Guidelines issued by DBOD to banks

Guidelines on 'Know Your Customer' norms and Anti-Money Laundering Measures- Extract

1. Introduction

The objective of KYC/AML/CFT guidelines is to prevent banks/FIs from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable banks/FIs to know/understand their customers and their financial dealings better and manage their risks prudently.

2. Definitions

2.1 Customer

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

2.2 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

2.3 “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.

2.4 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).

2.5 Transaction

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

(viii) opening of an account;
(ix) 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;

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

(xi) entering into any fiduciary relationship;

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

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

3. KYC Policy

Banks/FIs should frame their KYC policies incorporating the following four key elements:

(i) Customer Acceptance Policy (CAP);

(ii) Customer Identification Procedures (CIP);

(iii) Monitoring of Transactions; and

(iv) Risk Management.

3.1 Customer Acceptance Policy (CAP)

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

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

(ii) Parameters of risk perception are clearly defined in terms of the nature of business activity, location of the customer and his clients, mode of payments, volume of turnover, social and financial status, etc. so as to enable the bank/FIs in categorizing the customers into low, medium and high risk ones.

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

(iv) Not to open an account where the bank/FI is unable to apply appropriate customer due diligence measures, i.e., the bank/FI is unable to verify the

identity and /or obtain required documents either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The bank/FI may also consider closing an existing account under similar circumstances.

(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.

(vi) The bank/FI should have suitable systems in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanction lists circulated by the Reserve Bank.

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

3.2 Customer Identification Procedure (CIP)

3.2.1 General

(a) Customer identification means undertaking client due diligence measures while commencing an account-based relationship including identifying and verifying the customer and the beneficial owner on the basis of one of the OVDs. Banks/FIs need to obtain sufficient information to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of the banking relationship. ‘Being Satisfied’ means the bank/FI 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 the banks/FIs and a burdensome regime for the customers.

(b) Banks/FIs should have a policy approved by their Boards which should clearly spell out the Customer Identification Procedure to be carried out at different stages, i.e.,

(i) while establishing a banking relationship;

(ii) while carrying out a financial transaction;

(iii) when the bank/FI has a doubt about the authenticity or adequacy of the customer identification data it has obtained;

(iv) when banks sell third party products as agents;

(v) while selling banks' 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 a bank/FI has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000/-.

(c) Banks/FIs may 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 may be obtained separately after the account is opened only with the explicit consent of the customer.

3.2.2 Customer Due Diligence requirements (CDD) while opening accounts

A. Accounts of individuals:

(i) For opening accounts of individuals, banks/FIs should obtain one certified copy of an 'officially valid document' (as mentioned at paragraph 2.3 above) 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 by the bank/FI.

(ii) E-KYC service of Unique Identification Authority of India (UIDAI) should also be 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 to be 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 may be 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, banks/FIs should not insist on introduction for opening of bank accounts.

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

If an individual customer does not have any of the OVDs (as mentioned at paragraph 2.3 (i) above) as proof of identity, then banks/FIs are allowed 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 would be sufficient to obtain a certified copy of any one of the documents referred to

at proviso to paragraph 2.3 (i) above., which shall be deemed as an OVD for the purpose of proof of identity.

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

The additional documents mentioned at 2.3(ii) above shall be deemed to be OVDs under 'simplified measure' for the 'low risk' customers for the limited purpose of proof of address where customers are unable to produce any OVD for the same.

(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 2.3 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.

A 'small account' maybe opened on the basis of a self-attested photograph and affixation of signature or thumb print.

Such accounts may be opened and operated subject to the following conditions:

a) the designated officer of the bank, while opening the small account, certifies under his signature that the person opening the account has affixed her/his signature or thumb print, as the case may be, in her/his presence;

b) a small account shall be opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account and that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place;

c) a small account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the banking company 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) a small account shall be monitored and when there is suspicion of money laundering or financing of terrorism activity or other high risk scenarios, the identity of the customer shall be established through the production of “officially valid documents” and

e) foreign remittance shall not be allowed to be credited into a small account unless the identity of the customer 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 should 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, should 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 should 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/FI within a period of six months.

(x) In case of close relatives, e.g. husband, wife, son, daughter and parents, etc. who live with their wife, husband, father/mother, daughter and son, who do not have officially valid document for address verification, then, in such cases, banks/FIs

should 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.

(xi) Banks are not required to obtain fresh documents of customers when customers approach them for transferring their account from one branch of the bank to another branch of the same bank. Banks are advised that KYC verification once done by one branch of the bank should be valid for transfer of the account within the bank if full KYC verification has been done for the concerned account and is not due for periodic updation. The customers should be allowed to transfer their accounts 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 of a bank desires to open another account in the same bank, there should be no need for submission of fresh proof of identity and/or address.

(xii) Where a customer categorised 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 may 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, banks/FIs may rely on a third party subject to the conditions that-

1. the bank/FI immediately obtains necessary information of such client due diligence carried out by the third party;
2. the bank/FI 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/FI 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/FI is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable

3.3 Monitoring of Transactions

3.3.1 Ongoing monitoring

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

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

(b) Banks/FIs should pay particular attention to the following types of transactions:

(i) large and complex transactions, and those with unusual patterns, which have no apparent economic rationale or legitimate purpose.

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

(iii) transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer.

(iv) high account turnover inconsistent with the size of the balance maintained.

(c) Banks/FIs should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers should be carried out at a periodicity of not less than once in six months.

(d) Banks should closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies. Banks should analyse data in cases where a large number of cheque books are sought by the company, there are multiple small deposits (generally in cash) across the country in one bank account and where a large number of cheques are issued bearing similar amounts/dates. Where such features are noticed by the bank and in case they find such unusual operations in their accounts, the matter should be immediately reported to Reserve Bank and other appropriate authorities such as FIU-IND.

3.4 Risk Management

3.4.1 Banks/FIs should exercise on going due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge about the clients, their business and risk profile and where necessary, the source of funds.

The Board of Directors should ensure that an effective AML/CFT programme is in place by establishing appropriate procedures and ensuring their effective implementation. It should cover proper management oversight, systems and controls, segregation of duties, training of staff and other related matters. In addition, the following may also be ensured for effectively implementing the AML/CFT requirements.

(i) Using a risk-based approach to address management and mitigation of various AML/CFT risks.

(ii) Allocation of responsibility for effective implementation of policies and procedures.

(iii) Independent evaluation by the compliance functions of bank/FI's policies and procedures, including legal and regulatory requirements.

(iv) Concurrent/internal audit to verify the compliance with KYC/AML policies and procedures.

(v) Putting up consolidated note on such audits and compliance to the Audit Committee at quarterly intervals.

3.4.2 (a) Banks/FIs should prepare a profile for each new customer based on risk categorisation. 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/FI.

(b) Banks/FIs should categorise their customers into low, medium and high risk category based on their 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 banks/FIs are advised to have clear Board approved policies for risk categorisation and ensure that the same are meticulously complied with to effectively help in combating money laundering activities. 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, may be categorised 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, may also be classified as low risk customers.

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

The above guidelines for risk categorisation are indicative and banks/FIs may use their own judgement in arriving at the categorisation for each account based on their

own assessment and risk perception of the customers and not merely based on any group or class they belong to. Banks may use for guidance in their own risk assessment, the reports and guidance notes on KYC/AML issued by the Indian Banks Association.

4. General Guidelines

(i) **Confidentiality of customer information:**

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

(ii) **Avoiding hardship to customers:**

While issuing operational instructions to branches, banks/FIs should 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. Banks/FIs should, therefore, 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**

It may be appreciated that KYC norms/AML standards/CFT measures have been described 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/FIs as an integral part of their personnel recruitment/hiring process.

(v) **Employee training:**

Banks/FIs must 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 should be ensured.

(vi) **Provisions of FCRA**

Banks should 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 applies 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 **banks**/FIs 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***:*

Banks/FIs may nominate a Director on their Boards as “designated Director”, as required under 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 may be communicated to the FIU-IND. UCBs/ State Cooperative Banks /

Central Cooperative Banks can also designate a person who holds the position of senior management or equivalent as a 'Designated Director'. However, in no case, the Principal Officer should be nominated as the 'Designated Director'.

(x) **Principal Officer:**

Banks/FIs may appoint a senior officer as Principal Officer (PO). The PO should be independent and report directly to the senior management or to the Board of Directors. The PO shall 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 may be communicated to the FIU-IND.

II. Introduction of New Technologies – Credit Cards/Debit Cards/ Smart Cards/Gift Cards

Banks should pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent the same being used for money laundering purposes. Many banks are engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Banks should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. Banks are required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Further, marketing of credit cards is generally done through the services of agents. It is desirable that agents are also subjected to due diligence and KYC measures.

III Periodic updation of KYC

CDD requirements for periodic updation

Banks/FIs should carry out periodical updation of KYC information of every customer, which should include the following:

(i) KYC exercise should 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 may include all measures

for confirming the identity and address and other particulars of the customer that the bank/FI may consider 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) Banks/FIs need not seek fresh proofs of identity and address at the time of periodic updation, from those customers who are categorised 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 should suffice in such cases. In case of change of address of such ‘low risk’ customers, they could merely forward a certified copy of the document (proof of address) by mail/post, etc. Banks/FIs should not insist on physical presence of such low risk customer at the time of periodic updation. The time limits prescribed at (i) above would 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.

Annex-VII

Customer Identification Requirements – Indicative Guidelines

Beneficial ownership

When a bank/FI identifies a customer for opening an account, it should 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:

(f) 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-

3. *"Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the shares or capital or profits of the company.*
4. *"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.*

(g) 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.

(h) 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.

(i) 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.

(j) 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.

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

Trust/Nominee or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. In such cases, banks/FIs should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, banks/FIs should 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.

Accounts of companies and firms

(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.

Banks/FIs need to be vigilant against business entities being used by individuals as a ‘front’ for maintaining accounts with banks/FIs. Banks/FIs 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.

(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 may be required by the bank/FI to collectively establish the legal existence of such an association or body of individuals.

Client accounts opened by professional intermediaries

When the client **accounts** are opened **by professional intermediaries:** 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. Banks may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks, however, should not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the banks. 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 banks rely on the 'customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers. It should be understood that the ultimate responsibility for knowing the customer lies with the bank.

Accounts of Politically Exposed Persons (PEPs) resident outside India

Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Banks should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on such person in the public domain. Banks should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for a PEP should be taken at a senior level which should be clearly spelt out in the bank’s Customer Acceptance Policy. Banks should also subject such accounts to enhanced monitoring on an on-going basis. The above norms should also be applied to the accounts of the family members or close relatives of PEPs.

1) In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, banks should obtain senior

management's approval to continue the business relationship and subject the account to the CDD measures as applicable to PEPs including enhanced monitoring on an ongoing basis. These instructions are also applicable to accounts where a PEP is the ultimate beneficial owner.

Further, banks should have appropriate ongoing risk management systems for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner.

Accounts of non-face-to-face customers

With the introduction of phone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented should be insisted upon and, if necessary, additional documents may be called for. In such cases, banks may also require the first payment 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, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

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 may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc. Banks may 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) Such relationships may be established only with the approval of the Board, or by a Committee headed by the Chairman/CEO with clearly laid down parameters for approving such relationships, as approved by the Board. Proposals approved by the Committee should be put up to the Board at its next meeting for post facto approval.

(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) Banks 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) Banks should ensure that their 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) Banks should 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 should not permit its accounts to be used by shell banks.

xxx

Annex-VIII

Customer Identification Procedure

Documents that may be obtained from customers

Customers/Clients	Documents (Certified copy of any one of the following officially valid document)
Accounts of individuals - Proof of Identity and Address	Any one document from the Officially Valid Document is only allowed. They are: (i) Passport (ii) PAN card (iii) Voter's Identity Card issued by Election Commission (iv) Driving License (v) Job Card issued by NREGA duly signed by an officer of the State Govt (vi) 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 the following documents shall be deemed to be 'officially valid documents: i. 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; 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 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.
Accounts of Companies	(a) Certificate of incorporation; (b) Memorandum and Articles of Association; (c) A resolution from the Board of Directors and power of attorney granted to 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.
Accounts of Partnership firms	(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.
Accounts of Trusts and foundations	(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
Accounts of unincorporated association or a body of individuals	(a) Resolution of the managing body of such association or body of individuals; (b) Power of attorney granted to him 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 may be required by the bank to collectively establish the legal existence of such an association or body of individuals.
Accounts of Proprietorship Concerns Proof of the name, address and activity of the concern	Apart from Customer identification procedure as applicable to the proprietor any two of the following documents in the name of the proprietary concern would suffice • Registration certificate (in the case of a 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 the proprietary concern by any professional body incorporated under a statute. 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.

	In cases where the banks are satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the banks, however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern.

Annex IX

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

The e-KYC service of the UIDAI is be leveraged by NBFCs through a secured network. Any NBFC 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 NBFC to specifically access e-KYC service.

2. NBFCs 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 NBFC branches 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 use of e-KYC across various NBFC branches, as per UIDAI defined Application Programming Interface (API) protocols. For this purpose, NBFCs will have to develop their own software under the broad guidelines of UIDAI. Therefore, the software may differ from NBFC to NBFC.

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

5. Sample process flow would be as follows :

    a. Customer walks into branch of NBFC with **his / her 12-digit Aadhaar number and explicit consent** and requests to open a deposit account with

Aadhaar based e-KYC.

b. NBFC representative manning the branch enters the number into NBFC'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 Aadhaar 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 NBFC's e-KYC application and processed as needed.

g. NBFC'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, NBFCs decryption date and time stamp, etc.

h. The photograph and demographics of the customer can be seen on the screen of computer at NBFC branches for reference.

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

Appendix

List of KYC Circulars

Sr. No.	Circular No.	Date
i	DNBS (PD) CC.No.46/02.02(RNBC)/2004-05	December 30, 2004
ii	DNBS(PD). CC 48/10.42/2004-05	February 21, 2005
iii	DNBS(PD).CC No. 58/10.42/2005-06	October 11, 2005
iv	DNBS.PD. CC No. 64/03.10.042/2005-06	March 7, 2006
v	DNBS (PD). CC 113/03.10.042/2007- 08	April 23, 2008
vi	DNBS (PD). CC 163/03.10.042/2009- 10	November 13, 2009
vii	DNBS (PD).CC. No 166/03.10.42/2009-10	December 2, 2009
viii	DNBS. (PD) CC No 192/03.10.42/2010-11	August 9, 2010
ix	DNBS. (PD) CC No 193/03.10.42/2010-11	August 9, 2011
x	DNBS (PD).CC. No 201/03.10.42 /2010-11	September 22, 2010
xi	DNBS (PD).CC. No 202/03.10.42/2010-11	October 4, 2010
xii	DNBS(PD).CC.No209/03.10.42/2010- 11	January 28, 2011
xiii	DNBS(PD).CC.No210/03.10.42/2010-11	February 14, 2011
xiv	DNBS.(PD)CCNo212/03.10.42/2010-11	March 8, 2011
xv	DNBS(PD).CC. No.216/03.10.42/2010-11	May 02, 2011
xvi	DNBS(PD).CC.No218/03.10.42/2010-11	May 04 , 2011
xvii	DNBS.(PD)CC No215/03.10.42/2010-11	April 5, 2011
xviii	DNBS (PD).CC. No 242/03.10.42/2011-12	September 15, 2011
xix	DNBS (PD).CC. No 244/03.10.42/2011-12	September 22, 2011
xx	DNBS (PD).CC. No 251/03.10.42/2011-12	December 26, 2011
xi	DNBS (PD).CC. No 257/03.10.42/2011-12	March 14, 2012
xii	DNBS (PD).CC. No 264/03.10.42/2011-12	March 21, 2012
xiii	DNBS(PD).CC. No.270/03.10.42/2011-12	April 4, 2012
xiii	DNBS (PD).CC. No 275/03.10.42/2011-12	May 29, 2012
xiv	DNBS (PD).CC. No 294/03.10.42/2012-13	July 5, 2012
xv	DNBS (PD).CC. No 295/03.10.42/2012-13	July 11, 2012
xvi	DNBS (PD).CC. No 296/03.10.42/2012-13	July 11, 2012
xvii	DNBS (PD).CC. No 298/03.10.42/2012-13	July 26, 2012
xviii	DNBS (PD).CC. No 302/03.10.42/2012-13	September 7, 2012
ix	DNBS (PD).CC. No 304/03.10.42/2012-13	September 17, 2012
xx	DNBS (PD).CC. No 305/03.10.42/2012-13	October 3, 2012
xxi	DNBS (PD).CC. No 306/03.10.42/2012-13	October 3, 2012

xxii	DNBS (PD).CC. No 310/03.10.42/2012-13	November 22, 2012
xxiii	DNBS (PD).CC. No 313/03.10.42/2012-13	December 10, 2012
xxiv	DNBS (PD).CC. No 318/03.10.42/2012-13	December 28, 2012
xxv	DNBS (PD).CC. No 319/03.10.42/2012-13	December 28, 2012
xxvi	DNBS (PD).CC. No 321/03.10.42/2012-13	February 27, 2013
xxvii	DNBS (PD).CC. No 323/03.10.42/2012-13	April 18, 2013
xxviii	DNBS (PD).CC. No 324/03.10.42/2012-13	May 2, 2013
xxix	DNBS (PD).CC. No 325/03.10.42/2012-13	May 3, 2013
xxx	DNBS(PD).CC.No.351/03.10.42/2013-14	July 4, 2013
xxi	DNBS (PD).CC. No 352/03.10.42/2013-14	July 23, 2013
xii	DNBS(PD).CC.No 357/03.10.42/2013-14	October 3, 2013
xiii	DNBS(PD).CC NO 358/03.10.42/2013-14	October 3, 2013
xiv	DNBS(PD).CC.No.364/03.10.42/2013-14	January 1, 2014
xv	DNBS(PD).CC.No.366/03.10.42/2013-14	January 10, 2014
xvi	DNBS (PD).CC. No 370/03.10.42/2013-14	March 19, 2014
xvii	DNBS(PD).CC.No.375/03.10.42/2013-14	April 22 , 2014
xviii	DNBS (PD).CC. No 401/03.10.42/2014-15	July 25 , 2014
xix	DNBS (PD).CC. No 402/03.10.42/2014-15	August 1, 2014
xxxx	DNBS (PD).CC. No 404/03.10.42/2014-15	August 1, 2014
xi	DNBR.CC.PD.No.010/03.10.01/2014-15	January 09, 2015
xii	DNBR(PD).CC.No.034/03.10.42/2014-15	April 30, 2015

List of PMLA Circulars

Sr. No.	Circular No.	Date
i	DNBS (PD).CC 68/03.10.042/2005-06	April 5, 2006
ii	DNBS (PD).CC 126/03.10.042/2008-09	August 5, 2008
iii	DNBS (PD).CC 164/03.10.042/2009-10	November 13, 2009
iv	DNBS (PD).CC.No 170/03.10.42/2009-10	April 23, 2010
v	DNBS (PD).CC.No 171/03.10.42/2009-10	April 23, 2010
vi	DNBS (PD).CC.No 172/03.10.42/2009-10	April 30, 2010
vii	DNBS (PD).CC.No 175/03.10.42/2009-10	May 26, 2010
viii	DNBS (PD).CC.No 198/03.10.42/2010-11	August 26, 2010
ix	DNBS (PD).CC.No 247/03.10.42/2011-12	October 28, 2011
x	DNBS (PD).CC.No 307/03.10.42/2012-13	October 16, 2012
xi	DNBS (PD).CC.No 378/03.10.42/2013-14	May 29, 2014
xii	DNBS (PD).CC.No 398/03.10.42/2014-15	July 10, 2014
xiii	DNBS (PD).CC.No 400/03.10.42/2014-15	July 14, 2014
xiv	DNBS (PD).CC.No 401/03.10.42/2014-15	July 25, 2014
xv	DNBR (PD).CC.No 005/03.10.42/2014-15	December 01, 2014
xvi	DNBR CC.PD.No 009/03.10.01/2014-15	January 02, 2015
xvii	DNBR PD.CC.No 022/03.10.042/2014-15	March 16, 2015

*****