



भारतीय रिज़र्व बैंक

RESERVE BANK OF INDIA

www.rbi.org.in

RBI/2014-15/56

DNBS (PD) CC No. 387/03.10.42/ 2014-15

July 1, 2014

To

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

Dear Sirs,

**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 Master Circulars on various topics. In accordance with the approach, a master circular on the captioned subject, updated as on June 30, 2014 is being issued. The Master Circular has also been placed on the RBI web-site (<http://www.rbi.org.in>). A copy of the Master Circular is enclosed.

Yours faithfully,

(K. K. Vohra)  
Principal Chief General Manager

गैर बैंकिंग पर्यवेक्षण विभाग , केन्द्रीय कार्यालय, 2री मंजिल, सेन्टर I, वर्ल्ड ट्रेड सेंटर, कफ परेड, मुंबई-400 005  
फोन:22189131, फैक्स:22163768 ई-मेल: helpdnbs@rbi.org.in

Department of Non Banking Supervision, Central Office, 2<sup>nd</sup> Floor, Centre I, WTC, Cuffe Parade, Mumbai – 400 005  
Tel No: 22189131, Fax No: 22163768 Email: helpdnbs@rbi.org.in

हिंदी आसान है, इसका प्रयोग बढ़ाइए

## Table of Contents

Para No	Particulars
I	'Know Your Customer' (KYC) Guidelines - Anti Money Laundering Standards
	1 to 10- General
	11. Letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number
	12. Accounts of Politically Exposed Persons (PEPs)
	13. Client accounts opened by professional intermediaries
	14. Accounts of proprietary concerns
	15. Principal Officer
	16. Suspicion of money laundering/terrorist financing
	17. Filing of Suspicious Transaction Report (STR)
II	Prevention of Money Laundering Act, 2002 - Obligations of NBFCs in terms of Rules Notified thereunder
	1. General
	2. Maintenance of records of transactions
	3. Information to be preserved
	4. Maintenance and Preservation of records
	5. Reporting to Financial Intelligence Unit-India
	6 to 11- General
	12. PMLA Amendment rules 2009/2010
	13. Assessment and Monitoring of Risk
III	Combating financing of terrorism
IV	Operation of deposit account with NBFCs and money mules
	<b>Appendix</b>

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

1. 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. 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 not divulge any details thereof 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. 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. inasmuch 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.

4. In March, 2006, the KYC procedure 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, was further simplified.

5. 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 4 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.

6. 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) exceeds 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.

7. 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.

8. Permanent correct address, as referred to in Annex-VIII of this circular, means the address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other document accepted by the NBFC for verification of the address of the customer. In case utility bill is not in the name of

person depositing money but is close relative - wife, son, daughter and parents etc. who live with their husband, father/mother and son, NBFCs can obtain an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) wanting to open an account is a relative and is staying with him/her. 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.

**9.** 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. The periodicity of such updation should not be less than once in five years in case of low risk category customers and not less than once in two years in case of high and medium risk categories.

**10.** 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.

**11. 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.

**11A** <sup>1</sup>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 assets of Rs 25 cr and above and all Deposit taking NBFCs were advised to initiate steps for allotting Unique Customer Identification Code (UCIC) to all their customers while entering into any new relationships. Existing individual customers were also to be allotted UCIC by March 31, 2014. The UCIC will help NBFCs to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable NBFCs to have a better approach to

---

<sup>1</sup> Inserted vide DNBS (PD).CC. No. 325 /03.10.42 /2012-13 dated May 3, 2013

risk profiling of customers. It would also smoothen NBFCs operations for the customers.

## **12. 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.

## **13. 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 NBFCs 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.

#### **14. 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.

#### **15. Principal Officer**

NBFCs (including RNBCs) have been advised in Para 10 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 from time to time.

#### **16. 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.

#### **17. Filing of Suspicious Transaction Report (STR)**

In terms of Para 2 (iv) 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.

<sup>2</sup> 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.”*

---

<sup>2</sup> DNBS(PD).CC. No 378 /03.10.42 /2013-14 dated May 29, 2014

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.

## **2. Maintenance of records of transactions**

NBFCs should have a system of maintaining proper record of transactions prescribed under Rule 3, as mentioned below:

- (i) all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
- (ii) all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh;
- (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;
- (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.

## **3. Information to be preserved**

NBFCs are required to maintain the following information in respect of transactions referred to in Rule 3:

- (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.

## **4. Maintenance and 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. The identification records and transaction data should be made available to the competent authorities upon request.

- (i) In terms of Sub-Section 2(a) of Section 12 of The Prevention of Money Laundering (Amendment) Act, 2009 (PMLA, 2009), the records referred to in clause (a) of Sub-Section (1) of Section 12 shall be maintained for a period of ten years

from the date of transaction between the clients and the banking company and in terms of Sub-Section 2(b) of Section 12 of the Act *ibid*, the records referred to in clause (c) of Sub-Section (1) of Section 12 shall be maintained for a period of ten years from the date of cessation of transaction between the clients and the banking company.

(ii) NBFCs (including RNBCs) should maintain for at least ten years from the date of transaction between the NBFC (including RNBC) and the client, all necessary records of transactions referred to at Rule 3 of 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 (PMLA Rules), 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.

(iii) However, records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) obtained while opening the account and during the course of business relationship, as indicated in the paragraph, would continue to be preserved for at least ten years after the business relationship is ended as required under Rule 10 of the Rules *ibid*.

## **5. Reporting to Financial Intelligence Unit-India**

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.

6. 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>.

7. 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.

8. 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.

<sup>3</sup>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.

<sup>4</sup>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.

**9.** 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.

**10.** As stated in paragraph 4 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

<sup>3</sup> DNBS(PD).CC. No 307 /03.10.42 /2012-13 dated October 16, 2012

<sup>4</sup> Inserted vide DNBS(PD).CC.No.375/03.10.42/2013-14 dated April 22 , 2014

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.

**11.** 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.

**12. 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.

**13. 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 paragraph 2. 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 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.

<sup>5</sup>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

---

<sup>5</sup> Inserted vide DNBS(PD).CC.No.298/03.10.42 /2012-13 dated July 26, 2012

of suspicious activities contained in Annex-V of the CC No.126 dated August 05, 2008.

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 paragraph 4 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.

xxx

## 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

**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	<input type="checkbox"/> A <input type="checkbox"/> Cash Counter <input type="checkbox"/> D <input type="checkbox"/> RBI's CVPS	<input type="checkbox"/> B <input type="checkbox"/> Branch Level <input type="checkbox"/> Z <input type="checkbox"/> Other	<input type="checkbox"/> C <input type="checkbox"/> Currency Chest
3.5 Whether local police station has been informed	<input type="checkbox"/> Yes <input type="checkbox"/> 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 counterfeit 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 currency 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, police station etc., if available.

3.7 Mention additional 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 counterfeit 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.

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

**PART 2 STATISTICS**

2.1 Number of Counterfeit Currency Reports enclosed	<input type="text"/>
2.2 Total Value of Counterfeit Currency	<input type="text"/>

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 I)

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 institution, 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

1.	Introduction .....	2
2.	Counterfeit Currency Report .....	2
3.	Due Date .....	3
4.	Methods of filing .....	3
5.	Manual format .....	3
6.	Electronic format .....	3
7.	Description of Data Files .....	4
8.	Steps in preparation of data files .....	4
9.	Steps in validation /sufficiency of data files .....	4
10.	General Notes for all Data Files .....	4
11.	Data Structure of Control File (CCRCTL.txt) .....	5
12.	Data Structure of Branch File (CCRBRC.txt).....	7
13.	Data Structure of Transaction File (CCTRN.txt) .....	8

## 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  
Chanakypuri, 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:

- 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.
- 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:

- 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 ZipltFast 3.0 (or higher version) compression utility only to ensure quick and smooth acceptance of the file.
- 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 CCRTN.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 CCRTN.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.: 2 <sup>nd</sup> 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.: 2 <sup>nd</sup> 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	13 9	Y – for Yes, N – for No
17.	FIR Detail	CHAR	80	140	21 9	FIR, Police Station details etc., if available
18.	Additional Information	CHAR	80	220	29 9	Additional Information such as quality of counterfeit currency, sequence of events, if available
19.	Name of Tendering Person	CHAR	80	300	37 9	Person who tendered the counterfeit currency, if available.
20.	Name of Account Holder	CHAR	80	380	45 9	Name of the Sole/First account holder in whose account the counterfeit currency was tendered, if available.
21.	Account Number	CHAR	20	460	47 9	Account/Card Number of the person in whose account the counterfeit currency was tendered, if available.

### **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 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

## Guidelines issued by DBOD to banks

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

#### **'Know Your Customer' Standards**

1. The objective of KYC guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures also enable banks to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. Banks should frame their KYC policies incorporating the following four key elements:

- (i) Customer Acceptance Policy;
- (ii) Customer Identification Procedures;
- (iii) Monitoring of Transactions; and
- (iv) Risk management.

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

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

#### **Customer Acceptance Policy ( CAP )**

2. Banks should develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place on the following aspects of customer relationship in the bank.

- (i) No account is opened in anonymous or fictitious/ benami name(s);
- (ii) Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorization of customers into low, medium and high risk (banks may choose any suitable nomenclature viz. level I, level II and level III ); customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs – as explained in Annex II) may, if considered necessary, be categorised even higher;
- (iii) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and guidelines issued by Reserve Bank from time to time;

(iv) Not to open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non cooperation of the customer or non reliability of the data/information furnished to the bank. It may, however, be necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision to close an account may be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision;

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

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

Banks may prepare a profile for each new customer based on risk categorisation. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the bank. However, while preparing customer profile banks should take care to seek only such information from the customer which is relevant to the risk category and is not intrusive. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

For the purpose of risk categorisation, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorised as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government departments & Government owned companies, regulators and statutory bodies etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Customers that are likely to pose a higher than average risk to the bank may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Banks may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. Examples of customers requiring higher due diligence may include (a) non-resident customers, (b) high net worth individuals, (c) trusts, charities, NGOs and organizations receiving donations, (d) companies having close family shareholding or beneficial ownership, (e) firms with 'sleeping partners', (f) politically exposed persons (PEPs) of foreign origin, (g) non-face to

face customers, and (h) those with dubious reputation as per public information available, etc.

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

### **Customer Identification Procedure ( CIP )**

3. The policy approved by the Board of banks should clearly spell out the Customer Identification Procedure to be carried out at different stages i.e. while establishing a banking relationship; carrying out a financial transaction or when the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data. Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information. Banks need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship. Being satisfied means that the bank must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based approach is considered necessary to avoid disproportionate cost to banks and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc). For customers that are natural persons, the banks should obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the bank should (i) verify the legal status of the legal person/ entity through proper and relevant documents (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person, (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in Annex-II for guidance of banks. Banks may, however, frame their own internal guidelines based on their experience of dealing with such persons/entities, normal bankers' prudence and the legal requirements as per established practices. If the bank decides to accept such accounts in terms of the Customer Acceptance Policy, the bank 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. An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in the Annex-III.

<sup>6</sup>Rule 9(IA) of the Prevention of Money Laundering Rules, 2005 required every banking company, and financial institution, to identify the beneficial owner and take all reasonable steps to verify his identity. The term "beneficial owner" has been defined as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person. Government of India

---

<sup>6</sup> Inserted vide DNBS (PD).CC. No 321 /03.10.42 /2012-13 dated February 27, 2013

has since examined the issue and has specified the procedure for determination of Beneficial Ownership. The procedure as advised by the Government of India is as under:

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

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

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

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

B. Where the client is a trust, the banking company and financial institution, as the case may be, shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

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

All NBFCs/RNBCs were advised to review their KYC policy in the light of the above instructions and ensure strict adherence to the same.

### **Monitoring of Transactions**

4. Ongoing monitoring is an essential element of effective KYC procedures. Banks can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. Banks should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. The bank may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the bank. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts have to be subjected to intensified monitoring. Every bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of

funds, the type of transactions involved and other risk factors. Banks should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Banks should ensure that a record of transactions in the accounts is preserved and maintained as required in terms of section 12 of the PML Act, 2002. It may also be ensured that transactions of suspicious nature and/ or any other type of transaction notified under section 12 of the PML Act, 2002, is reported to the appropriate law enforcement authority. Banks should ensure that its branches continue to maintain proper record of all cash transactions ( deposits and withdrawals) of Rs.10 lakh and above. The internal monitoring system should have an inbuilt procedure for reporting of such transactions and those of suspicious nature to controlling/ head office on a fortnightly basis.

### **Risk Management**

5. The Board of Directors of the bank should ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It should cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility should be explicitly allocated within the bank for ensuring that the bank's policies and procedures are implemented effectively. Banks may, in consultation with their boards, devise procedures for creating Risk Profiles of their existing and new customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or banking/business relationship.

Banks' internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Banks should ensure that their audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Concurrent/ Internal Auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard may be put up before the Audit Committee of the Board on quarterly intervals.

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

### **Customer Education**

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

## **Introduction of New Technologies – Credit cards/debit cards/smart cards/gift cards**

7. 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 their use in money laundering schemes.

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. Further, marketing of these cards is generally done through the services of agents. Banks should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that agents are also subjected to KYC measures.

**In case of NBFCs this policy may be adopted in respect of issue of credit cards as NBFCs are not permitted to issue debit cards, smart cards, stored value cards, charge cards, etc.**

### **KYC for the Existing Accounts**

8. Banks were advised vide our circulars DBOD.AML.BC.47/14.01.001/2003-04, DBOD.AML.129/14.01.001/2003-04 and DBOD.AML.BC.No.101/14.01.001/ 2003-04 dated November 24, 2003, December 16, 2003 and June 21, 2004 respectively to apply the KYC norms advised vide our circular DBOD. No. AML.BC.18/ 14.01.001/ 2002-03 dated August 16, 2002 to all the existing customers in a time bound manner. **[NBFCs were advised, vide our circular DNBS(PD) CC No. 34/2003-04 dated January 6, 2004 to apply the KYC norms to all the existing customers in a time bound manner.]** While the revised guidelines will apply to all new customers, banks should apply the same to the existing customers on the basis of materiality and risk. However, transactions in existing accounts should be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the CDD measures. Banks may consider applying monetary limits to such accounts based on the nature and type of the account. It may, however, be ensured that all the existing accounts of companies, firms, trusts, charities, religious organizations and other institutions are subjected to minimum KYC standards which would establish the identity of the natural/legal person and those of the 'beneficial owners'. Banks may also ensure that term/ recurring deposit accounts or accounts of similar nature are treated as new accounts at the time of renewal and subjected to revised KYC procedures.

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

### **Applicability to branches and subsidiaries outside India**

9. The above guidelines shall also apply to the branches and majority owned subsidiaries located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of Reserve Bank.

### **Appointment of Principal Officer**

10. Banks may appoint a senior management officer to be designated as Principal Officer. Principal Officer shall be located at the head/corporate office of the bank and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism.



**Customer Identification Requirements – Indicative Guidelines**

**Trust/Nominee or Fiduciary Accounts**

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Banks should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, banks may insist on receipt of 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. While opening an account for a trust, banks should take reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

**Accounts of companies and firms**

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

**Client accounts 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 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 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 through to 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 regulated and supervised and has adequate systems in place to comply with the KYC requirements. 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 or of 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 the 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 PEP should be taken at a senior level which should be clearly spelt out in Customer Acceptance policy. Banks should also subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

### **Accounts of non-face-to-face customers**

With the introduction of telephone 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 may 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**

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 should gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Information on the other bank's 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 correspondent's/respondent's country may be of special relevance. Similarly, banks should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. While it is desirable that such relationships should be established only with the approval of the Board, in case the Boards of some banks wish to delegate the power to an administrative authority, they may delegate the power to a committee headed by the Chairman/CEO of the bank while laying down clear parameters for approving such relationships. Proposals approved by the Committee should invariably be put up to the Board at its next meeting for post facto approval. The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented. In the 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. The correspondent bank should also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

Banks should refuse to 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 unaffiliated to any regulated financial group). Shell banks are not permitted to operate in India. Banks should also guard against establishing relationships with respondent foreign financial institutions that permit their accounts to be used by shell banks. Banks should be extremely cautious while continuing relationships with respondent banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing. Banks should ensure that their respondent banks have anti money laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

xxx

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

<b>Features</b>	<b>Documents</b>
<p>Accounts of individuals</p> <p>Legal name and any other names used</p> <p>Correct permanent address</p>	<p>(i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving licence (v) Identity card (subject to the bank's satisfaction) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of bank</p> <p>(i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority</p> <p>(iv) Electricity bill (v) Ration card</p> <p>(vi) Letter from employer (subject to satisfaction of the bank)</p> <p>( any one document which provides customer information to the satisfaction of the bank will suffice )</p>
<p>Accounts of companies</p> <ul style="list-style-type: none"> <li>- Name of the company</li> <li>- Principal place of business</li> <li>- Mailing address of the company</li> <li>- Telephone/Fax Number</li> </ul>	<p>(i) Certificate of incorporation and Memorandum &amp; Articles of Association (ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf (iv) Copy of PAN allotment letter (v) Copy of the telephone bill</p>
<p>Accounts of partnership firms</p> <ul style="list-style-type: none"> <li>- Legal name</li> <li>- Address</li> <li>- Names of all partners and their addresses</li> <li>- Telephone numbers of the firm and partners</li> </ul>	<p>(i) Registration certificate, if registered</p> <p>(ii) Partnership deed (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf</p> <p>(iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses</p> <p>(v) Telephone bill in the name of firm/partners</p>
<p>Accounts of trusts &amp; foundations</p> <ul style="list-style-type: none"> <li>- Names of trustees, settlers, beneficiaries and signatories</li> </ul>	<p>(i) Certificate of registration, if registered</p> <p>(ii) Power of Attorney granted to transact business on its behalf</p>

<ul style="list-style-type: none"> <li>- Names and addresses of the founder, the managers/directors and the beneficiaries</li> <li>- Telephone/fax numbers</li> </ul>	<ul style="list-style-type: none"> <li>(iii) Any officially valid document to identify the trustees, settlors, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses</li> <li>(iv) Resolution of the managing body of the foundation/association</li> <li>(v) Telephone bill</li> </ul>
<p>Accounts of Proprietary Concerns</p> <p>-Name, Address and Activity of the Proprietary Concern.</p>	<ul style="list-style-type: none"> <li>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 &amp; 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.</li> <li>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.</li> <li>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.</li> <li>iv) Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern.</li> <li>v) Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.</li> </ul>

## Appendix

### List of KYC Circulars

Sr. No.	Circular No.	Date
(i)	<a href="#">DNBS (PD) CC.No.46/02.02(RNBC)/2004-05</a>	December 30, 2004
(ii)	<a href="#">DNBS(PD). CC 48 /10.42/2004-05</a>	February 21, 2005
(iii)	<a href="#">DNBS(PD).CC No. 58/ 10.42 /2005-06</a>	October 11, 2005
(iv)	<a href="#">DNBS.PD. CC No. 64 /03.10.042/2005-06</a>	March 7, 2006
(v)	<a href="#">DNBS(PD). CC 113 /03.10.042/ 2007- 08</a>	April 23, 2008
(VI)	<a href="#">DNBS(PD). CC 163/03.10.042/ 2009- 10</a>	November 13, 2009
(vii)	<a href="#">DNBS(PD).CC. No 166 /03.10.42 /2009-10</a>	December 2, 2009
(viii)	<a href="#">DNBS. (PD) CC No 192 /03.10.42/2010-11</a>	August 9, 2010
(ix)	<a href="#">DNBS. (PD) CC No 193 /03.10.42/2010-11</a>	August 9, 2011
(x)	<a href="#">DNBS(PD).CC. No 201/03.10.42 /2010-11</a>	September 22, 2010
(xi)	<a href="#">DNBS(PD).CC. No 202 /03.10.42 /2010-11</a>	October 4, 2010
(xii)	<a href="#">DNBS(PD).CC.No209/03.10.42/2010-</a>	January 28, 2011
(xiii)	<a href="#">DNBS(PD).CC.No210/03.10.42/2010-11</a>	February 14, 2011
(xiv)	<a href="#">DNBS.(PD)CCNo212/03.10.42/2010-11</a>	March 8, 2011
(xv)	<a href="#">DNBS(PD).CC. No.216 /03.10.42 /2010-11</a>	May 02, 2011
(xvi)	<a href="#">DNBS(PD).CC.No218/03.10.42/2010-11</a>	May 04 , 2011
(xvii)	<a href="#">DNBS.(PD)CC No215/03.10.42/2010-11</a>	April 5, 2011

(xviii)	<a href="#">DNBS(PD).CC. No 242 /03.10.42 /2011-12</a>	September 15, 2011
xix	<a href="#">DNBS(PD).CC. No 244 /03.10.42 /2011-12</a>	September 22, 2011
xx	<a href="#">DNBS(PD).CC. No 251 /03.10.42 /2011-12</a>	December26, 2011
xi	<a href="#">DNBS(PD).CC. No 257 /03.10.42 /2011-12</a>	March 14, 2012
xii	<a href="#">DNBS(PD).CC. No 264/03.10.42/2011-12</a>	March 21, 2012
xiii	<a href="#">DNBS(PD).CC. No.270/03.10.42 /2011-12</a>	April 4, 2012
xiii	<a href="#">DNBS(PD).CC. No 275 /03.10.42 /2011-12</a>	May 29, 2012
xiv	<a href="#">DNBS(PD).CC. No 294 /03.10.42 /2012-13</a>	July 5, 2012
xv	<a href="#">DNBS(PD).CC. No 295 /03.10.42 /2012-13</a>	July 11, 2012
xvi	<a href="#">DNBS(PD).CC. No 296 /03.10.42 /2012-13</a>	July 11, 2012
xvii	<a href="#">DNBS(PD).CC. No 298 /03.10.42 /2012-13</a>	July 26, 2012
xviii	<a href="#">DNBS(PD).CC. No 302 /03.10.42 /2012-13</a>	September 7,2012
ix	<a href="#">DNBS(PD).CC. No 304 /03.10.42 /2012-13</a>	September 17,2012
xx	<a href="#">DNBS(PD).CC. No 305 /03.10.42 /2012-13</a>	October 3,2012
xxi	<a href="#">DNBS(PD).CC. No 306 /03.10.42 /2012-13</a>	October 3,2012
xxii	<a href="#">DNBS(PD).CC. No 310 /03.10.42 /2012-13</a>	November 22,2012
xxiii	<a href="#">DNBS(PD).CC. No 313 /03.10.42 /2012-13</a>	December 10, 2012
xxiv	<a href="#">DNBS(PD).CC. No 318 /03.10.42 /2012-13</a>	December 28, 2012

xxv	<a href="#">DNBS(PD).CC. No 319 /03.10.42 /2012-13</a>	December 28, 2012
xxvi	<a href="#">DNBS(PD).CC. No 321 /03.10.42 /2012-13</a>	February 27,2013
xxvii	<a href="#">DNBS(PD).CC. No 323 /03.10.42 /2012-13</a>	April 18, 2013
xxviii	<a href="#">DNBS(PD).CC. No 324 /03.10.42 /2012-13</a>	May 2, 2013
xxix	<a href="#">DNBS(PD).CC. No 325 /03.10.42 /2012-13</a>	May 3, 2013
xxx	<a href="#">DNBS(PD).CC.No.351/03.10.42/2013-14</a>	July 4, 2013
xxi	<a href="#">DNBS(PD).CC. No 352/03.10.42 /2013-14</a>	July 23, 2013
xii	<a href="#">DNBS(PD).CC.No 357/03.10.42/2013-14</a>	October 3.2013
xiii	<a href="#">DNBS(PD).CC NO 358/03.10.42/2013-14</a>	October 3, 2013
xiv	<a href="#">DNBS(PD).CC.No.364/03.10.42/2013-14</a>	January 1, 2014
xv	<a href="#">DNBS(PD).CC.No.366 /03.10.42/2013-14</a>	January 10, 2014
xvi	<a href="#">DNBS (PD).CC. No 370 /03.10.42 /2013-14</a>	March 19, 2014
xvii	<a href="#">DNBS(PD).CC.No.375/03.10.42/2013-14</a>	April 22 , 2014

### List of PMLA Circulars

Sr. No.	Circular No.	Date
(i)	<a href="#">DNBS(PD). CC 68 /03.10.042/2005-06</a>	April 5, 2006
(ii)	<a href="#">DNBS(PD). CC 126/03.10.042/ 2008- 09</a>	August 5, 2008
(iii)	<a href="#">DNBS(PD). CC 164/03.10.042/ 2009- 10</a>	November 13, 2009
(iv)	<a href="#">DNBS(PD).CC. No 170 /03.10.42 /2009-10</a>	April 23 , 2010
(v)	<a href="#">DNBS(PD)CC.No 171/03.10.42/2009-10</a>	April 23 , 2010
(vi)	<a href="#">DNBS(PD).CC. No. 172 /03.10.42 /2009-10</a>	April 30, 2010
(vii)	<a href="#">DNBS(PD)CC.No 175/03.10.42/2009-10</a>	May 26, 2010
(ix)	<a href="#">DNBS(PD)CC.No 198 /03.10.42/2010-11dated</a>	August 26, 2010
(x)	<a href="#">DNBS(PD).CC. No 247 /03.10.42 /2011-12</a>	October 28, 2011
(xi)	<a href="#">DNBS(PD).CC.No.307/03.10.42/2012-13</a>	October 16 , 2012
(xii)	<a href="#">DNBS(PD).CC. No 378 /03.10.42 /2013-14 May 29, 2014</a>	May 29, 2014

\*\*\*\*\*