RBI/2009-10/9

DNBS (PD) CC No. 151/03.10.42/ 2009-10 **July 1, 2009**

To

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

Dear Sir,

Master Circular – 'Know Your Customer' (KYC) Guidelines – Anti Money Laundering Standards

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 up to 30th June 2009 is being issued. It may be noted that the Master Circular consolidates and updates all the instructions contained in the notifications listed in the Appendix, in so far they relate to the subject. 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 sincerely,

(P. Krishnamurthy)
Chief General Manager-in-Charge

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

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 has 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-1. These guidelines are equally applicable to NBFCs. All NBFCs are, 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 within three months of the date of this circular. NBFCs were advised to ensure that they are fully compliant with the instructions before December 31, 2005.

2. While preparing operational guidelines NBFCs may 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.

(Details are in DNBS (PD). CC 48 /10.42/2004-05 dated February 21, 2005)

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 NBFC and persons authorised by NBFCs including brokers/agents etc.**

An obligation has been cast on the banking companies, financial institutions and intermediaries, by the Prevention of Money Laundering Act, 2002 (Chapter IV), to comply with certain requirements in regard to maintenance of record of the transactions of prescribed nature and value, furnishing of information relating to those transactions and verification and maintenance of the records of identity of all its clients in prescribed manner. Accordingly, instructions were issued to NBFCs vide our circular DNBS (PD) CC No. 48 /10.42/ 2004-05 dated February 21, 2005.

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 should 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. Compliance in this regard were to be reported to RBI by December 31, 2005.

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. The companies may also evolve suitable review procedures to identify persons authorised by NBFCs including brokers/agents etc. in whose cases the incidence of discontinued deposits is high for taking suitable action.

(Details are in DNBS (PD). CC No.58 / 10.42 / 2005-06 dated October 11, 2005)

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

4. It was clarified in March 2006 that although flexibility in the requirement of documents of identity and proof of address has been provided in the circular mentioned above yet there may be instances where certain persons, especially, those belonging to low income group both in urban and rural areas may not be able to produce such documents to satisfy the NBFC about their identity and address. Hence, it has been decided to further simplify 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.

5. Accordingly, in case a person who wants to open an account is not able to produce documents mentioned in Annexure II of DBOD circular enclosed with our circular dated February 21, 2005, NBFCs may open accounts as described in paragraph 2 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.

(Details are in DNBS (PD). CC No.64 / 03.10.042 / 2005-06 dated March 7, 2006)

7. It was further clarified to NBFCs in April 2008 that for the purpose of Circular dated February 21, 2005 the term **'being satisfied'** 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 was also given in the Annex-III to this circular. It may happen that Annex-III, 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 are, therefore, advised to take a review of their extant internal instructions in this regard.

8. It is clarified that permanent correct address, as referred to in Annex-III 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. NBFCs are further advised that such review of risk categorisation of customers should be carried out at a periodicity of **not less** than once in six months. NBFCs also 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. NBFCs have been further advised in terms of extant instructions that KYC/AML guidelines issued by Reserve Bank of India shall also apply to their 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. It is further clarified that 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. **Combating financing of terrorism**

a) In terms of PMLA Rules, suspicious transaction should include *inter alia* transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. NBFCs are, 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.

b) 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.

12. 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.

13. In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, NBFCs may consider the indicative list of suspicious activities contained in Annex-V of the CC No.126 dated August 05, 2008.

14. These guidelines are issued under Sections 45K and 45L of the Reserve Bank of India Act, 1934 and any contravention of or non-compliance with the same may attract penalties under the relevant provisions of the Act.

(Details are in DNBS (PD). CC No.113 /03.10.42 / 2007-08 dated April 23, 2008)

xxx

Annex-1

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.

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.

<u>Risk Management</u>

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.

<u>Applicability to branches and subsidiaries outside India</u>

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.

<u>Appointment of Principal Officer</u>

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.

Annex-II

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 identify 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

<u>Annex-III</u>

Customer Identification Procedure

Features to be verified and documents that may be obtained from customers

Features	**Documents**
Accounts of individuals	
Legal name and any other names used	(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
Correct permanent address	(i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority (iv) Electricity bill (v) Ration card (vi) Letter from employer (subject to satisfaction of the bank) (any one document which provides customer information to the satisfaction of the bank will suffice)
Accounts of companies - Name of the company - Principal place of business - Mailing address of the company - Telephone/Fax Number	(i) Certificate of incorporation and Memorandum & 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

Accounts of partnership firms - Legal name - Address - Names of all partners and their addresses - Telephone numbers of the firm and partners	(i) Registration certificate, if registered (ii) Partnership deed (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses (v) Telephone bill in the name of firm/partners
Accounts of trusts & foundations - Names of trustees, settlers, beneficiaries and signatories - Names and addresses of the founder, the managers/directors and the beneficiaries - Telephone/fax numbers	(i) Certificate of registration, if registered (ii) Power of Attorney granted to transact business on its behalf (iii) Any officially valid document to identify the trustees, settlors, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses (iv) Resolution of the managing body of the foundation/association (v) Telephone bill

Appendix

List of Circulars

Sr. No.	Circular No.	Date
(i)	DNBS (PD) CC.No.46/02.02(RNBC)/2004-05	December 30, 2004
(ii)	DNBS(PD). CC 48 /10.42/2004-05	February 21, 2005
(iii)	DNBS(PD).CC No. 58/ 10.42 /2005-06	October 11, 2005
(iv)	DNBS.PD. CC No. 64 /03.10.042/2005-06	March 7, 2006
(v)	DNBS(PD). CC 113 /03.10.042/ 2007- 08	April 23, 2008