‘Know Your Customer’ Guidelines
Anti Money Laundering Standards

1. Know Your Customer Standards

a) The objective of the KYC guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures enable banks to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. The revised KYC policy of the bank incorporates the following four elements:

i. Customer Acceptance Policy (CAP)
ii. Customer Identification Procedures (CIP)
iii. Monitoring of Transactions; and
iv. Risk Management

b) A customer for the purpose of KYC Policy is defined as:

- A person or entity that maintains an account and/or has a business relationship with the bank
- One on whose behalf the account is maintained (i.e., the beneficial owner)
- Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors, etc as permitted under the law
- 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 high value demand draft as a single transaction.

2. Customer Acceptance Policy (CAP)

a) The following Customer Acceptance Policy indicating the criteria for acceptance of customers shall be followed in the bank. The branches shall accept customer strictly in accordance with the said policy:

i. No account shall be opened in anonymous or fictitious/benami name(s)

ii. Parameters of risk perception shall be 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 called Level I, Level II and Level III respectively; Customers requiring very high level of monitoring e.g., Politically Exposed Persons (PEPs) may be categorized as Level IV.

iii. The branches shall collect documents and other information from the customer depending on perceived risk and keeping in mind the requirements of AML Act, 2002 and guidelines issued by RBI from time to time

iv. The branches shall close an existing account or shall not open a new account where it is unable to apply appropriate customer due diligence measures i.e., branch is unable to verify the identity and/or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of data/information furnished to the branch. The branches shall, however, ensure that these measures do not lead to the harassment of the customer. However, in case the account is required to be closed on this ground, the branches shall do so only after permission of J/DGM (I&V) of their concerned Zonal Offices is obtained. Further, the customer should be given a prior notice of at least 20 days wherein reasons for closure of his account should also be mentioned.

v. The Updated Manual of Instructions (Chapter 2 Volume I) provides detailed guidelines as to the mode of operations of different types of accounts and the circumstances in which a customer is permitted to act on behalf of another person/entity. The branches are advised to strictly follow these instructions.

vi. The branches shall make 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. RBI has been circulating lists of terrorist entities notified by the Government of India so that banks exercise caution against any transaction detected with such entities. The branches shall invariably consult such lists to ensure that prospective person/s or organizations desirous to establish relationship with the bank are not in any way involved in any unlawful activity and that they do not appear in such lists.

b) The branches shall prepare a profile for each new customer based on risk categorization. The bank has devised a revised Composite Account Opening Form for recording and maintaining the profile of each new customer. Revised form is separate for Individuals, Partnership Firms, Joint Customers, Corporates and other legal entities or special accounts e.g., account in the name of brand names, domain names, etc. The nature and extent of due diligence shall depend on the risk perceived by the branch. The branches should continue to follow strictly the instructions issued by the bank regarding secrecy of customer information. The branches should bear in mind that the adoption of customer acceptance policy and its implementation does not become too restrictive and should not result in denial of banking services to general public, especially to those, who are financially or socially disadvantaged.

c) The risk to the customer shall be assigned on the following basis:

i. Low Risk (Level I):

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 categorized as low risk. The illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and

Government owned companies, regulators and statutory bodies etc. In such cases, only the basic requirements of verifying the identity and location of the customer shall be met.

ii. Medium Risk (Level II):

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; such as:

a) Persons in business/industry or trading activity where the area of his residence or place of business has a scope or history of unlawful trading/business activity.
b) Where the client profile of the person/s opening the account, according to the perception of the branch is uncertain and/or doubtful/dubious.

iii. High Risk (Level III):

The branches 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. The 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.

The persons requiring very high level of monitoring may be categorized as **Level IV**.

3. Customer Identification Procedure (CIP)

a) Customer identification means identifying the person and verifying his/her identity by using reliable, independent source documents, data or information. The branches 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 branch is able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance of the extant guidelines in place. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc). For customers that are natural persons, the branches shall 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 branches shall (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 Annexure I for the guidance of branches.

b) If the branch decides to accept such accounts in terms of the Customer Acceptance Policy, the branch shall 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 Annexure – II.

4. Monitoring of Transactions

a) Continuous monitoring is an essential ingredient of effective KYC procedures and the extent of monitoring should be according to the risk sensitivity of the account. Branches shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Transactions that involve large amount of cash inconsistent with the size of the balance maintained may indicate that the funds are being 'washed' through the account. High risk accounts shall be subjected to intensive monitoring.

b) The branches shall continue to follow strictly the instructions regarding cash transactions issued vide our Circular No.326 reference No. BDS&P/MRC/2003-1980 dated 05.03.2003, wherein a threshold limit of Rs.5 lakh for cash transactions and Rs.10 lakh for fund transfer transactions was set for reporting details thereof. However, as per revised KYC policies and procedures, the branches are now required to maintain proper record of all cash transactions (both deposits and withdrawals) of Rs.10 lakh and above only. The details of cash transactions involving deposits and withdrawals of Rs.10 lakh and above are to be furnished to the concerned Joint General Manager/Deputy General Manager (I&V), Zonal Offices on fortnightly basis viz., as on every 15th and last working day of the month containing full particulars such as name of the account holder, account number, date of opening of account and other details as mentioned in Circular No.74/95 reference No. BDS&P/878/95/460 dated 25.08.1995 and reiterated vide Circular No.168 reference No. PDA/CPPD-01/02-18 dated 27.09.2002 and Circular No.326 reference No.BDS&P/MRC/2003-1980 dated 05.03.2003. These statements have to reach the concerned JGM/DGM (I&V), Zonal Office within seven days from the stipulated date of the fortnightly statement.

c) The I&V Department, Corporate Headquarters shall ensure adherence to the KYC policies and procedures. Concurrent/Internal Auditors shall specifically check and verify the application of KYC procedures at the branches and comment on the lapses if any observed in this regard. The compliance in this regard shall be put up before the Audit Committee of the Board on quarterly intervals. All staff members shall be provided training on Anti Money Laundering as conveyed vide Circular No.326 reference No. BDS&P/MRC/2003-1980 dated 05.03.2003. The focus of training shall be different for frontline staff, compliance staff and staff dealing with new customers.

5. Risk Management

a) The bank's KYC policies and procedures covers management oversight, systems and controls, segregation of duties, training and other related matters. For ensuring effective implementation of the bank's KYC polices and procedures, the Branch Managers shall explicitly allocate responsibilities within the branch. The Branch Manager shall authorize the opening of all new accounts. However, in case of branches with business of Rs.50 crore or above, where there is usually another senior Officer next below the Branch Manager heading the Accounts Department

may authorize the opening of new accounts. The branches shall prepare risk profiles of all their existing and new customers and apply Anti Money Laundering measures keeping in view the risks involved in a transaction, account or banking/business relationship.

b) Training encompassing applicable money laundering laws and recent trends in money laundering activity as well as the bank's policies and procedures to combat money laundering shall be provided to all the staff members of the bank periodically in phases. The HRD Department, Corporate Headquarters shall determine the frequency of training and identify personnel to be trained at each branch.

c) The General Manager, Planning & Accounts Department shall be empowered to prescribe threshold limits for a particular group of accounts and the branches shall pay particular attention to the transactions which exceed these limits. The threshold limits shall be reviewed annually and changes, if any, conveyed to branches for monitoring.

d) The bank's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The compliance function shall provide an independent evaluation of the bank's own polices and procedures, including legal and regulatory requirements. The bank shall ensure that the audit machinery of the bank is staffed adequately with individuals who are well versed in such policies and procedures. Concurrent/Internal Auditors shall 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 shall be put up before the Audit Committee of the Board on quarterly intervals.

6. Customer Education

Implementation of KYC procedures requires branches to demand certain information from the customers that may be of personal in nature or which have hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. Therefore, the front desk staff needs to handle such situations tactfully while dealing with customers and educate the customer of the objectives of the KYC programme. The branches shall also be provided specific literature/pamphlets to educate customers in this regard.

7. New Technologies

The KYC procedures shall invariably be applied to new technologies including 'JK Bank Global Access Debit Card' products and/or 'JK Bank Credit Card' products, including Internet banking/Mobile banking facility or such other product which may be introduced by the bank in future that might favour anonymity, and take measures, if needed to prevent their use in money laundering schemes. Branches should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that if at any point of time bank appoints/engages agents for marketing of these cards / products are also subjected to KYC measures.

8. KYC for the Existing Accounts

As per extant RBI guidelines, the branches were required to obtain **Composite Account Opening Form** from all the existing customers as per the following schedule:

		Date for

S.No./ Category	Nature of customer accounts	Completion of the Process
1.	All types of customer accounts including borrowal accounts of the companies, firms, trusts, institutions etc.	March 31, 2004
2.	All customer accounts including borrowal accounts, other than those included in category 1 above, opened during the period from January1, 1998 till date	June 30, 2004
3.	All customer accounts including borrowal accounts, other than those included in category 1 above, opened between January 1, 1993 and December 31, 1997	September 30, 2004
4.	All customer accounts including borrowal accounts, other than those included in category 1 above, opened before January 1, 1993.	December 31, 2004

While, the revised guidelines shall apply to all new customers/accounts, branches shall apply these to the existing customers on the basis of materiality and risk. However, transactions in existing accounts shall be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the Customer Due Diligence (CDD) measures. It has however to be ensured that all the existing accounts of companies, firm, trusts, charitable, 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'. **The term/recurring deposit accounts or accounts of similar nature shall be treated as new accounts at the time of renewal and shall be subjected to revised KYC procedures.**

9. Appointment of Principal Officer

To ensure compliance, monitoring and report compliance of Anti Money Laundering policy of the bank, Senior Executive heading the I&V Department of the bank at Corporate Headquarters shall act as Principal Officer. He shall be responsible to monitor and report transactions and share information on Anti Money Laundering as required under the law. The Principal Officer shall maintain close liaison with enforcement agencies, banks and any other institutions that are involved in the fight against money laundering and combating financing of terrorism. The Principal Officer shall furnish a compliance certificate to the Board on quarterly basis certifying that Revised Anti Money laundering Policy is being strictly followed by all the branches of the bank.

Annex- I

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. The branches should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, branches shall 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, branches 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

Branches need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. Branches 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. But at least promoters, directors and its executives need to be identified adequately.

Client accounts opened by professional intermediaries

When the branch 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. Branches may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Branches should 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 branch and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such accounts are co-mingled at the branch, the branch should still look through to the beneficial owners. Where the bank rely on the 'customer due diligence' (CDD) done by an intermediary, it shall satisfy itself that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements.

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. Branches 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. Branches should verify

the identify of the person and seek information about the sources of funds before accepting the PEP as a customer. The branches should seek prior approval of their concerned Zonal Heads for opening an account in the name of PEP.

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 shall be insisted upon and, if necessary, additional documents may be called for. In such cases, branches may also require the first payment to be effected through the customer's account if any 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 branches might 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

a) 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. The bank while entering into any kind of correspondent banking arrangement shall 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 shall be of special relevance. Similarly, the bank shall also ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. Such relationships shall be established only with the prior approval of the Board. The Board may in the alternative delegate powers in this regard to a committee headed by the Chairman/CEO of the bank and lay 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 bank shall also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

b) Bank shall not enter into a correspondent relationship with a 'shell bank'. A Shell bank is 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. Bank shall also guard against establishing relationships with respondent foreign financial institutions that permit their accounts to be used by "shell banks". The Bank shall move

cautiously 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 policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts

Annex-II

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 satisfaction of the branch) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of branch (vii) Telephone bill (viii) Bank account statement
• Correct permanent address	(ix) Letter from any recognized public authority (x) Telephone bill (xi) Bank account statement (xii) Letter from any any recognized public authority xiii) Electricity Bill

	xiv) Ration Card xv) Letter from the employer, (subject to the satisfaction of the branch) xvi) Any other 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