Group Anti Money Laundering Policy

April 2008

INDEX

1 Preamble

1.a) Background

Money Laundering (ML) is the processing of criminal proceeds in order to disguise their illegal origin. Banking system worldwide is susceptible to channeling of funds for such activities. In response to the international community's growing concern about this problem, most global organisations and national governments who are members of the United Nations General Assembly have been actively pursuing programs to deter ML and following are the major developments in this regard:

Developments in India

Reserve Bank of India (RBI), the regulator of banks in India has issued detail guidelines to Banks on Know Your Customer (KYC) and Anti Money Laundering (AML) in November 2004.

The Indian Parliament passed the Prevention of Money Laundering Act (PMLA) in 2002 to implement the Political Declaration adopted by the special session of the United Nations General Assembly held during June 8-10, 1998 and the Global Programme of Action annexed to Resolution S-17/2 adopted by the United Nations General Assembly on February 23, 1990. The provisions of this Act are effective from July 1, 2005. The PMLA addresses a range of issues including the definition of and punishment for the offence of ML, attachment and confiscation of property tainted by ML and the obligations of banking companies, financial institutions and intermediaries in connection with ML issues.

Under PMLA, the scope of ML covers certain offences under the Narcotics Drugs and Psychotropic Substances Act, 1985, the Indian Penal Code, 1860, the Arms Act, 1959, the Wild Life (Protection) Act, 1972, the Immoral Traffic (Prevention) Act, 1956 and the Prevention of Corruption Act, 1988.

The Government of India had notified on July 1, 2005, the rules under Prevention of Money Laundering Act, 2002 (PMLA) relating to "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" (hereinafter referred to as "PMLA Rules"). In terms of the requirement of the PMLA Rules, procedures for furnishing of information (relating to specified transactions) to the Financial Intelligence Unit, India (FIU-IND) have been notified by Reserve Bank of India on February 15, 2006.

International Developments

The Financial Action Task Force (FATF), which is a body promoted by thirty-one nations and two international organisations has recommended AML requirements for commercial and other banking institutions.

The Government of United States of America (US) has enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (the "Patriot Act") Act of 2001, which has a far-reaching impact on international banking and cross border transactions.

The Basel Committee on Banking Supervision has stipulated guidelines on consolidated KYC Risk Management and Customer Due Diligence.

Various other countries have enacted laws/regulations to deal with the threat of ML. These include Proceeds of Crime Act (POCA) in United Kingdom and Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTF) in Canada.

The US regulators have also brought into effect the Customer Identification Program Rules (CIP Rules) under Section 326 of the Patriot Act. US banks having dealings with banks outside the US are required to ensure substantial compliance with the provisions of CIP Rules by the international banks, in their dealings with the US banks.

1.b) ICICI Bank's initiatives

ICICI Bank Limited (hereinafter referred to as the "Bank") constantly benchmarks itself against international practices, regulations and conventions to the extent reasonable and practicable. The Bank had therefore undertaken a comprehensive review of its AML framework and laid down a Group Anti Money Laundering Policy in January 2004 which is reviewed from time to time. The basic purpose of the Group AML Policy is to establish a global AML framework (including Know Your Customer aspects) for the Bank to participate in the international efforts against ML and ensure that the Bank is not used as a vehicle for ML. The AML framework of the Bank would meet the extant regulatory requirements.

1.c) Scope

The Group AML Policy establishes the standards of AML compliance and is applicable to all activities of the Bank including its Strategic Business Units (SBUs) in India or abroad. For the purpose of this Policy, the term 'SBUs' refers to any business group constituted by the Bank for carrying out its activities/offering of the Bank's products and services and otherwise as may be specified for the purpose of AML compliance monitoring by the Money Laundering Reporting Officer (MLRO) of the Bank. The functions of MLRO are outlined later in Section 6(c) of this Policy.

Detailed KYC/AML procedures for SBUs for different products/services would be laid down in line with the Group AML Policy with the approval of the Product

and Process Approval Committee (PAC) of the Bank. However, if it is observed that any country/jurisdiction has any peculiar/unique AML requirements, overseas SBUs are required to implement such standards and accordingly adopt appropriate AML Policy/procedures for the same. Such AML Policy/procedures shall be an addendum to this Group AML Policy (to be read in conjunction with the Group AML Policy) and would be applicable only to the respective overseas SBUs. These addendums would be approved by the PAC.

The Group AML Policy framework enshrined in this document would be used by the subsidiaries of ICICI Bank, including its overseas subsidiaries and joint ventures/alliances. The subsidiaries/joint ventures/alliances shall formulate their respective AML policies (in line with their regulatory requirements) with the approval of the respective Board of Directors/Committee of Directors and in consultation with the MLRO of the Bank. Such policy documents may cover the AML Procedures as well.

A glossary of terms important to the Group AML Policy is given in Annexure I.

2 Group AML Policy Objectives

Within the overall Group AML Policy framework, the key AML objectives of the Bank are:

- To prevent the Bank's business channels/products/services from being used as a channel for ML.
- To establish a framework for adopting appropriate AML procedures and controls in the operations/business processes of the Bank.
- To ensure compliance with the laws and regulations in force from time to time.
- To protect the Bank's reputation.
- To assist law enforcement agencies in their effort to investigate and track money launderers.
- To lay down AML compliance norms for the employees of the Bank.

3 Definition of Money Laundering

ML is the process by which criminals attempt to disguise the true origin of the proceeds of their criminal activities by the use of the financial system so that after a series of transactions, the money, its ownership and the income earned from it appear to be legitimate. According to FATF, ML is the processing of criminal proceeds in order to disguise their illegal origin.

This process is often achieved by converting the original illegally obtained proceeds from their original form, usually cash, into other forms such as deposits or securities and by transferring them from one financial institution to another using the account of apparently different persons or businesses.

Section 3 of PMLA, describes the offence of ML. Section 3 reads as under:

"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering."

3.a) Money Laundering Cycle

The process of ML, regardless of its degree of complexity, is accomplished in three stages, namely the placement stage, layering stage and integration stage.

Placement Stage

This involves the physical movement of the cash proceeds. For most criminal transactions, cash is the most common medium of exchange and criminals who accumulate large volumes of cash are the most vulnerable to detection and seizure. As a result, money launderers will attempt, through placement, to channel the funds into a bank.

Layering Stage

After the funds enter a bank, the money launderer will further separate the illicit proceeds from their illegal source through a process of layering. Layering occurs by conducting multiple, complex, financial transactions that make it difficult to link the money to an illegal activity. Layering disguises or eliminates the audit trail.

Integration Stage

During this process the money launderer will integrate the illicit funds into the economy by providing what appears to be a legitimate explanation for his or her illicit financial wealth. For example, integration of these proceeds might include the purchase of real estate, businesses, securities, automobiles or jewellery. Integration moves the funds back into the economy with the appearance of being normal business earnings. It would become extremely difficult at this point for a bank to distinguish between illicit funds and legitimate funds.

3.b) Money Laundering Risks

The Bank is aware that it is exposed to several risks if an appropriate AML framework is not established:

Reputation Risk- Risk of loss due to severe impact on Bank's reputation. This may be of particular concern given the nature of the Bank's business, which requires maintaining the confidence of depositors, creditors and the general marketplace.

Compliance Risk- Risk of loss due to failure of compliance with key Regulations governing the Bank's operations.

Operations Risk- Risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

Legal Risk- Risk of loss due to any of the above risk or combination thereof resulting into the failure to comply with Law and having a negative legal impact on the Bank. The specific types of negative legal impacts could arise by way of fines, confiscation of illegal proceeds, criminal liability etc.

Financial Risk- Risk of loss due to any of the above risks or combination thereof resulting into the negative financial impact on the Bank.

4 AML Standards

The Bank would adopt a risk-based approach in implementing its AML framework. The AML standards of the Bank would be primarily based on two pillars, namely, KYC and Monitoring/Reporting of Suspicious Transactions (MSTR). The suspicious transactions shall include large as well as cash transactions above a threshold limit as per applicable regulations/Bank's internal guidelines and shall be monitored and reported. Detailed procedure manuals shall be prepared for each SBU illustrating the KYC and MSTR requirements for the various products.

4.a) Risk-based approach in implementing AML framework

In order to ensure efficient implementation of the AML framework by the SBUs, it is necessary to establish a risk-based process on the basis of which SBUs shall evolve detailed AML procedures specific to their activity. It is recognised that a higher level of due diligence and monitoring would be specified for business areas prone to higher ML risks.

Accordingly, individuals 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 (ex: customers with well defined salary structures). Further, customers that are like to pose a higher than average risk to the bank may be categorised as medium or high risk depending on factors such as customer's backgrounds, nature and location of activity etc. Wherever relevant, the product segments would also be categorised based on the ML risk as per the guidelines of RBI.

4.b) Customer Risk Caterorisation

RBI, vide its guidelines dated February 18, 2008, required banks to undertake and periodically review Customer Risk Categorisation (CRC). Further, the customer identification data is also required to be updated by the banks periodically based on the CRC. Appropriate operational instructions would be issued by the MLRO of the Bank, from time to time, in this regard. These operational instructions would also include specifying appropriate measures for review of CRC and updation of customer identification data as per applicable guidelines.

Based on the above, the SBUs would devise appropriate risk-based KYC/transaction monitoring procedures and would put up the same for the approval by the PAC.

The Bank shall not deal with Shell Banks (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group) and would guard against establishing relationship with Foreign Banks, which permit their accounts to be used by shell banks. The Bank would be cautious in dealing with Foreign Banks located in the Non-Cooperative Countries and Territories (NCCT) as outlined in Annexure I.

Further, all the correspondent banking relationships with the counter party banks would be approved by the COD in accordance with the parameters laid down in the Know Your Customer (KYC) procedures formulated for Correspondent Banking relationships, internally from time to time.

4.c) Know Your Customer (KYC)

The Bank is aware that availability of sufficient customer information underpins all other AML procedures and should be seen as a critical element in the effective management of ML risks.

Keeping in view the specific requirements of the guidelines of RBI, the Bank has evolved a Customer Acceptance Policy (CUSTAP) (Refer Annexure II) which lays down the criteria for the acceptance of Customers. The CUSTAP would form an integral part of the Group AML Policy. The aspects mentioned in the CUSTAP would be reckoned while evolving the KYC/AML procedures for various customers/products.

The KYC procedures would be based on the following principles in addition to the various aspects outlined in the CUSTAP:

- In dealing with customers across various geographies, product lines (including those utilizing new technologies) and business segments, the Bank is aware that the ML risks may vary. Therefore the Group AML Policy requires adoption of a risk-based KYC procedure to be evolved separately for various business segments in line with the international best practices.

- The Bank shall ensure that there is in place a process of customer identification and verification depending on the nature/status of the customer and kind of transactions that are contemplated to take place at the respective SBUs.

- Appropriate customer identification and verification procedures (basic/ enhanced due diligence as highlighted in the CUSTAP) shall be conducted by SBUs at different stages i.e. while establishing a banking relationship, carrying out a financial transaction or when the Bank has doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

- Each SBU shall ensure that a business relationship is commenced only after establishing and verifying the identity of the customer and understanding the nature of the business the customer expects to conduct.

- The risk based KYC procedures adopted by the SBUs shall be applicable to all the new customer relationships.

- The KYC procedures shall become applicable to existing customers only if the risk profile of the customer or customer segment changes to a higher risk category or based on materiality or pursuant to any applicable regulatory guidelines or when there is an unusual pattern in the operation of account. This shall be done by way of enhanced due diligence.

- The Bank shall obtain information from correspondent banks as regards their compliance with an acceptable AML program in order to proceed with offering its services to the customers of the correspondent bank.

- The Bank shall ensure that while processing incoming wire transfers (cross border and domestic), the remitter information is made available as part of wire transfers. The Bank ensures adherence to appropriate internal procedures devised to operationalise this requirement.

- Appropriate KYC procedures based on commercial judgment shall be adopted by the relevant SBUs which will include systems relating to proper management oversight, controls, segregation of duties, training, due diligence, reporting, regulations and other related procedures.

4.d) Monitoring/Reporting of Suspicious Transactions (MSTR)

Ongoing monitoring of accounts is an essential element of an effective AML framework. A Suspicious Transaction is one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of account. A satisfactory KYC procedure provides the foundation for recognising unusual or suspicious transactions. Knowledge of the customer's normal or expected activities would enable the Bank to recognise when a transaction or series of transactions are abnormal. Accounts categorized as high risk accounts shall be subject to intensified monitoring. Sufficient guidance/training shall be imparted to staff to enable them to recognise potentially suspicious transactions. However considering the magnitude of the transactions being handled, it would be necessary to develop appropriate software systems to identify and report suspicious transactions. The assessment of suspicious transaction shall be based on a reasonable evaluation of relevant factors, including having information on the client's business, financial history, background, behaviour and threshold limits for transactions as stipulated by applicable regulations/Bank's internal guidelines. As a part of ongoing monitoring, transactions of individuals/entities shall be screened against negative list, including those notified by regulators/statutory authorities.

The Bank would endeavour to implement appropriate systems so as to:

- Ensure that the SBUs have in place requisite processes and technology to:

- Monitor transactions in order to identify unusual behaviour
- Upon such identification, to conduct enhanced due diligence
- Based on the results of such enhanced due diligence, to report any suspicious transaction which has been identified.

- Establish Management Information Systems (MIS) to identify critical areas and issues which need to be addressed to prevent ML and to provide required information relating to suspicious transactions to the top management and regulatory authorities at pre-determined intervals.

- To have proper record maintenance policies and procedures, which would ensure that documents required are available within reasonable time frame. Each SBU shall develop appropriate parameters for transaction monitoring and suspicious behaviour in consultation with the MLRO. The country and product specific details of likely or potentially suspicious transactions such as large transactions and cash transactions shall be included in specific AML Procedures along with the threshold limits as defined by respective regulations and/or internal guidelines.

5 AML Procedures

5.a) Formulation of AML Procedures

All SBUs shall formulate business/product specific AML procedures which include systems for due diligence for identification of risks, compliance with applicable laws etc.

The detailed AML procedures would cover the following areas:

Product risk rating: All SBUs shall assign a product risk rating based on identified parameters.

Customer risk rating: Segments of customers shall be rated based on their perceived ML risks.

Risk based KYC procedures: The KYC procedures shall be based on perceived product and customer segment risk and cover the complete spectrum of activities during customer acquisition such as identification procedures, verification of documents and account opening.

Product wise ML indicators at account opening stage: These indicators will enable the SBUs to monitor the customer acquisition process at the initial stage itself.

Transaction Monitoring: The details of transactions prone to ML risks shall be adequately described and a framework for monitoring of transactions and reporting suspicious transactions shall be laid down. Adequate guidance to staff to recognise suspicious customer behaviour shall be outlined. Parameters to be continuously tracked through system support shall be laid down. Measures of enhanced due diligence for identifying suspicious transactions from the unusual transactions would be laid down.

Reporting structure: The structure for reporting unusual and suspicious transactions and ML activities shall be laid down.

Internal controls: Internal control processes for appropriate escalation procedures and periodic audits shall be laid down.

5.b) Role of employees

The Human Resource Policy of the Bank and all its SBUs shall include the due diligence procedures from an AML perspective that need to be carried out before employing any personnel including temporary or outsourced manpower. Keeping in view the new regulatory guidelines of RBI, the due diligence procedure would also include name screening of prospective employees against the list of terrorists / individuals / entities provided by RBI.

The role of employees in implementing any AML framework being critical, employees would be expected to carry out the stipulated procedures efficiently. Any inefficient or suspicious behaviour of employees shall be dealt with suitably. The employees shall maintain strict confidentiality in regard to KYC, MSTR and other AML procedures.

If any activity is outsourced to any agency/individual, it would be ensured that they would adhere to the guidelines outlined in this Policy.

5.c) Training

Adequate ongoing training programmes shall be conducted for all employees on the requirements laid down in this Policy document as well as the KYC/AML procedures.

Specialised training programmes shall be undertaken to address the needs of:

- MLRO, the SBU Compliance functionaries and their staff.
- The employees dealing with high ML risk products.
- The employees with customer contacts or those authorised to settle cash or non-cash financial transactions.

The AML training programmes shall address the requirements relating to the following:

- AML requirements.
- Possible risks of not adhering to the AML requirements.
- Requirements for adequate KYC procedures.
- Methods for recognition of suspicious transactions or suspicious behaviour of a client.

Training must relate to employees' daily work and comprise examples from business including continuous training needs.

6 AML Operating Structure

6.a) Audit Committee

The Audit Committee shall supervise the implementation of the Group AML Policy framework.

6.b) Product and Process Approval Committee (PAC)

All the new products and processes, after evaluation from the ML risk perspective, would be approved by the PAC. PAC would also approve appropriate AML/KYC procedures (including the policies/procedures related to overseas jurisdictions) applicable for various SBUs taking into account the risk-based approach outlined in Section 4(a) above.

6.c) Compliance Group (CG)

Compliance Group would be responsible for:

- Formulating and periodically reviewing the Group AML Policy in line with the applicable regulatory guidelines.

- Ensuring that the regulatory guidelines are incorporated in the AML related procedures put in place by the FCPRRMG (specified below).

- Instituting a risk-based AML training programme at the Group.

6.d) Financial Crime Prevention and Reputation Risk Management Group (FCPRRMG) and the Money Laundering Reporting Officer (MLRO)

In order to have a focused attention to Financial Crime Prevention, a separate team headed by the MLRO of the Bank has been constituted. The activities of FCPRRMG include establishing appropriate internal controls, procedures and systems in regard to Fraud Prevention, Anti Money Laundering (AML) etc.

MLRO is a senior level officer of the Bank, who has the executive responsibility for monitoring day-to-day implementation of the Group AML Policy and Procedures. The functions of the MLRO shall include:

- Liaising with the regulatory/enforcement authorities on AML matters. MLRO shall submit periodic reports to the Audit Committee including the adequacy of the systems and controls of SBUs for managing ML risks and for recommending any changes or improvements, as necessary.

- Review and approve all products/services offered by the SBUs to ensure compliance with AML policies and procedures. All SBUs shall refer all their respective products and services to MLRO in this regard at the time of putting them for approval of the PAC.

- Ensure that AML controls are put in place before any new product is launched. The controls shall include the ML risk rating of product, checklist on ML

indicators, definition of suspicious behaviour and compliance framework and systems for monitoring and mitigating the ML risks.

- Participate in strategic planning meetings or comment on proposed plans specifically if the new strategy increases the ML risk exposure of the SBUs e.g. expansion into international markets, introduction of products to facilitate cross border payments etc.

- Advise the detailed responsibilities of the respective AML Compliance functionaries in consultation with the respective SBU Heads from time to time.

- Review all reports required to be submitted to regulatory/law enforcement authorities

- Reporting to the FIU-IND

    - Cash Transaction Report – On a monthly basis before 15th of the succeeding month

    - Suspicious Transaction Report - within seven days from the date of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of integrally connected are of suspicious nature.

- Monitoring of compliance and exception reporting.

6.e) Anti Money Laundering Compliance Function at SBUs

Each SBU Head shall be responsible to implement the AML framework, policies and procedures in his/her respective SBU. To aid effective implementation, each SBU shall have a designated official to perform AML compliance function, which will operate independently and report, identified suspicious transactions, if any, to the MLRO. The compliance function shall draw upon the expertise from the risk, compliance, legal and system functions.

The SBU compliance functionary shall be responsible for:

- ML risk monitoring, risk measurement and risk evaluation at the SBU.
- Ensuring that the MIS is generated as per the internal policies and regulatory requirements.
- Providing inputs to employees/managers of the SBUs on issues related to ML risks.
- Ensuring that there are comprehensive, updated operating risk management procedures in line with this policy to guide the day-to-day activities of SBUs.
- Collating and maintaining the AML records.
- Ensuring the validity and accuracy of the data used for AML analysis.
- Monitoring of compliance and exceptions reporting.
- Escalation of unusual behaviour and suspicious activity/transactions to MLRO.
- Participation in the development of behaviour tracking models and operations of AML system.

- Co-ordination and participation with sub-groups, which are set up from time to time to study specific matters.
- Making specific requests to MLRO for training, systems upgradation etc.

6.f) Escalation Procedures

All SBUs shall escalate any identified suspicious activity or transaction to the MLRO as soon as possible but not later than one working day after establishing the reasonable grounds for suspicion.

The MLRO shall report to the FIU-IND all suspicious activities/transactions in accordance with the PMLA rules, within seven days from the date of arriving at such conclusion that any transaction, whether cash or non-cash, or a series of integrally connected are of suspicious nature.

7 MIS & Reporting

7.a) Record Keeping

The Bank shall maintain appropriate documentation on their customer relationships and transactions to enable reconstruction of any transaction.

The records shall be maintained for a period of ten years from the date of cessation of the transaction. Records shall be maintained in a manner, which facilitates its easy retrieval as and when required.

7.b) Reporting to Audit Committee of the Board

The Audit Committee shall review reports detailing the ML risk management actions of the Bank and its subsidiaries.

Adequacy of the ML risk measurement systems, including any findings of internal and external auditors and advisors shall be reported to the Audit Committee on a quarterly basis.

7.c) Reporting Procedures for Subsidiaries

The reporting procedures for Subsidiaries would be laid down by the MLRO of the Bank. The report would contain information, inter alia, in respect of deficiencies in compliance with procedures, a summary of latest changes in ML preventive guidelines or other regulations, information on training provided to staff members during the period, any resources requirements, information concerning reports from Reporting Accountants or Internal Audit and a risk assessment of the impact of new products/services.

7.d) Regulatory Reporting

All SBUs must implement necessary procedures and controls to ensure that all regulatory reporting as laid down by the applicable regulations is completed properly and within the required reporting timelines.

The MLRO or his designated staff shall review all reports required to be submitted to regulatory/law enforcement authorities prior to submission from time to time.

Each SBU must use specific forms/formats as approved by the MLRO for reporting unusual transactions/suspicious transactions or in submitting any other information as may be prescribed.

8 Compliance

8.a) Internal Controls

The Group AML Policy adopts the following controls:

- Appropriate organisation structure (definitions of duties and responsibilities, discretionary limits for approval and decision making procedures).

- Adequate internal controls (segregation of various functions, cross-checking, dual control, double signatures, etc). These controls shall be supplemented by an effective audit function that independently evaluates the adequacy, operational effectiveness and efficiency of the control systems within the organisation.

- Duties and responsibilities shall be explicitly allocated at SBUs for ensuring that policies and procedures are managed effectively and that there is full commitment and compliance to an effective KYC programme in respect of both existing and prospective accounts.

- MLRO along with the SBU Heads shall periodically monitor strict adherence to the policies and procedures by the officials.

8.b) Audit/Monitoring

The scope of internal audit of the Bank shall include testing of compliance with the Group AML Policy and KYC/AML procedures by the various SBUs. The checklist of items reviewed, including a summary of deficiencies and actions taken must be documented and submitted to the Audit Committee.

The Bank shall monitor all Large Transactions and Cash Transactions beyond the threshold limits as defined by the MLRO of the Bank and updated periodically to the PAC.

8.c) Co-operative Efforts

As a part of its risk management strategy, the Bank shall co-operate with regard to the law enforcement and mutual assistance programmes initiated by various countries as may be required under applicable laws in India or other laws governing the SBUs.

8.d) Customer Education

The Bank shall educate the customers on the objectives of KYC/AML related programmes of the Bank, by way of preparation of specific literature/pamphlets, hosting relevant KYC/AML information on the website of the Bank etc.

8.e) Updation

Given the fact that the risks the Bank faces are constantly changing and that ML risk management methodologies, regulations and tools are also evolving, it is imperative that this policy document be reviewed on annual basis or earlier when there are significant changes in the applicable AML regulations.

Annexure I

Glossary of Terms

Banking

As per Banking Regulation Act, 1949 "banking" means the accepting, for the purpose of lending or investment, of deposits of money from the public, repayable on demand or otherwise and withdrawable by cheque, draft, order or otherwise. For the purpose of this policy," banking" shall also include any activity permitted under the Banking Regulation Act, 1949.

Customer

The term 'Customer' would refer to any person or entity whether a natural person, juristic entity, a firm, a trust, an unincorporated association of persons, acting for itself or in any fiduciary capacity, who (i) for itself or on behalf of another, maintains an account or (ii) has a business relationship with the Bank for availing any of the products or services of the Bank or (iii) is a beneficiary of the transactions conducted by Professional Intermediaries [Professional Intermediaries include Stockbrokers, Chartered Accountants, Solicitors etc. as permitted under law or customary practices] or (iv) is connected with a financial transaction which can pose significant reputational or other risks to the Bank.

Account

"Account" is defined generally as any formal business relationship established to effect financial transactions.

Proceeds of Crime

The term 'proceeds of crime' shall mean any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a offence covered by PMLA or the value of any such property.

Records

The term 'Records' shall include the records maintained in the form of books or stored in a disk, floppy/micro film etc. and any other electronic storage device or such other form as may be prescribed.

Offence of Money Laundering

The term 'Offence of Money Laundering' shall have the meaning ascribed to the term under PMLA which is: "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of Money Laundering".

Transaction – Rule 2(1)(h) of the PMLA Rules

Transaction includes deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means.

Suspicious Transaction – Rule 2(1)(g) of the PMLA Rules

Suspicious transaction is a transaction whether or not made in cash which to a person acting in good faith

(a) gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
(b) appears to be made in circumstances of unusual or unjustified complexity; or
(c) appears to have no economic rationale or bonafide purpose; or
(d) give rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;

Based on the above, it may be observed that suspicious transactions or activities are activities where the economic background of the customer or any transacting party and/or the purpose of any transaction or business relationship in its form or amount appears unusual or suspicious in relation to the customer, or the relevant products/services or the concerned location of the Bank, or if the economic purpose or legality of the transaction is not immediately clear. The parameters to establish suspicious transactions such as:

- Account activities not consistent with the customer's business or normal transaction profile of the customer.
- Transactions which attempts to avoid reporting/record-keeping requirements.
- Unusual activities.
- Transaction or account activities pertaining to customer who provides insufficient or suspicious information or is reluctant to provide requisite information.
- Suspicious fund transfer activities.

FATF

The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental body whose purpose is the development and promotion of policies to combat ML.

The FATF currently consists of thirty-one countries and two international organisations. Its membership includes the major financial centre countries of Europe, North and South America and Asia.

Non-Cooperative Countries and Territories (NCCT)

As defined by the Financial Action Task Force (FATF) as countries with no or insufficient Anti-Money Laundering measures. However, currently there are no NCCTs that are notified by the FATF.

Shell Bank

Shell Bank is a bank, which does not have a physical presence in any country and is unaffiliated to any regulated financial group. The term `physical presence' means a place of business that (i) is maintained by a bank; (ii) is at a fixed address (other than solely an electronic address) in a country in which the bank is authorised to conduct banking activities, at which location the bank employs one or more individuals on a full-time basis and maintains operating records related to its banking activities; and (iii) is subject to inspection by the banking authority, which licensed the bank to conduct banking activities.

Annexure II

Customer Acceptance Policy

Preamble

ICICI Bank (hereinafter referred to as "Bank") has already formulated a Group Anti Money Laundering (AML) Policy, which establishes the standards of AML compliance and is applicable to all activities of the Bank. The Group AML Policy highlights Know Your Customer (KYC) as one of the key AML standards. The availability of customer information is a critical element in the effective management of Money Laundering (ML) risks. The Group AML policy as well as the KYC/AML procedures already laid down by the Bank, cover the aspects of customer identification/verification, the due diligence procedures to be adopted and in general the Bank's overall policy in regard to acceptance of customers or establishing a relationship. However, keeping in view the requirements of the recent guidelines of Reserve Bank of India (RBI) titled "Know Your Customer Guidelines – Anti Money Laundering Standards", dated November 29, 2004, it is now felt that a separate Customer Acceptance Policy for the Bank be formulated which lays down the criteria for acceptance of customers. The Customer Acceptance Policy would form an integral part of the Group AML Policy. The features of the Customer Acceptance Policy are detailed below.

Definition of Customer

The term 'Customer' would refer to any person or entity whether a natural person, a juristic entity, a firm, a trust, an unincorporated association of persons, acting for itself or in any fiduciary capacity, who (i) for itself or on behalf of another, maintains an account or (ii) has a business relationship with the Bank for availing any of the products or services of the Bank or (iii) is a beneficiary of the transactions conducted by Professional Intermediaries [Professional Intermediaries include Stockbrokers, Chartered Accountants, Solicitors etc. as permitted under law or customary practices] or (iv) is connected with a financial transaction which can pose significant reputational or other risks to the Bank.

Due Diligence for Account Opening/Closing

- The Bank shall not open any account(s) in anonymous or fictitious/benami name(s). Adequate due diligence is a fundamental requirement for establishing the identity of the customer. Identity generally means a set of attributes which together uniquely identify a natural person or legal entity. In order to avoid fictitious and fraudulent applications of the customers, and to achieve a reasonable degree of satisfaction as to the identity of the customer, Strategic Business Units (SBUs) shall conduct appropriate basic due diligence. The nature and extent of basic due diligence measures to be conducted by the SBUs at the time of establishment of account opening/relationship, would be dependent upon the risk category of the customers and involve the collection and recording of information (including those as may be prescribed by the regulators, if any) by using reliable independent documents, data or any other information. This may include identification and verification of the applicant and wherever relevant, ascertaining of occupational details, legal status, ownership and control structure and any additional information in line with the assessment of the ML risks posed

by the applicant and the applicant's expected use of the bank's products and services. In case of certain products, the Bank may rely upon the KYC procedures conducted by other Banks having satisfactory customer identification procedures.

For non-face to face customers, appropriate due diligence measures (including certification requirements of documents, if any) will be devised by the SBUs for identification and verification of such customer. The purpose of commencing the relationship/opening of accounts shall be established and the beneficiary of the relationship/account shall also be identified. The due diligence measures to be adopted for various customer/product segments shall be outlined in the respective KYC/AML procedures laid down from time to time. The information collected from the customer shall be kept confidential.

- Appropriate Enhanced Due Diligence measures shall be adopted for customers, with a high-risk profile, especially those for whom the sources of funds are not clear, transactions carried through correspondent accounts and customers who are Politically Exposed Persons (PEPs) resident outside India and their family members/close relatives. 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. The KYC/AML procedures shall also specify that after gathering sufficient information including the source of funds, the decision to open an account for PEPs shall be taken at a reasonably senior level in the Bank. Such accounts shall be subject to enhanced monitoring on an ongoing basis. In respect of unusual or suspicious transactions/applications or when the customer moves from a low risk to a high-risk profile, appropriate enhanced due diligence measures shall be adopted. The enhanced due diligence measures to be adopted for various customer/product segments shall be outlined in the respective KYC/AML procedures laid down from time to time.

- The Bank shall 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. or any other internal negative lists of the Bank.

- The Bank shall not open an 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 due to non cooperation of the customer or non reliability of the data/information furnished to the Bank. On the same grounds, if the Bank is not able to apply appropriate customer due diligence measures on an existing account, the Bank shall take steps to close the account. However, the decision to close an existing account shall be taken by the respective Head of Business Group, after giving due notice to the customer explaining the reasons for such a decision.

Risk Profiling of customer/product segments

- The Bank has adopted a risk-based approach in implementing its AML framework as spelt out in the Group AML Policy of the Bank. This approach includes

assessment of various risks associated with different types of customer/product segments.

- The customer/product segments shall be categorised into high, medium and low risk categories, depending upon the perceived ML risks and customer behaviour. For the purpose of risk categorisation, customer segments comprising such individuals 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. Appropriate ML risk indicators (including those relating to customer's background, nature and location of activity, country of origin, sources of funds and client profile etc.) shall be analysed for categorisation of customer segments into medium/high risk. Customer segments that are likely to pose a higher than average risk to the Bank may be categorized as medium or high-risk. The risk categorization of the customers shall be reviewed periodically. Appropriate ML risk parameters shall be considered for categorization of product segments, which shall be laid down in the KYC/AML procedures for different products.

- The SBUs of the Bank shall conduct risk profiling of the various customer segments periodically and submit the risk profile to the Money Laundering Reporting Officer (MLRO). The customer profile may contain information relating to customer’s identity, social/financial status, nature of business activity, information about clients’ business and their location etc. The MLRO shall approve the risk profiles with such changes thereto as may be required in consultation with the respective SBUs.

- The Bank may prepare a profile of the customer based on available information. Considering the large volumes of business, it would be necessary that appropriate software systems would have to be developed to capture the individual customer profile information, especially for high risk customers. The customer profile information shall be a confidential document.

Documentation

- The Bank shall obtain satisfactory evidence of the identity of the customer depending upon the perceived risks at the time of commencement of relationship/opening of account. Such evidences shall be substantiated by reliable independent documents, data or information or other means like physical verification etc. In order to avoid customer inconvenience, under special circumstances, the Bank may rely on certain data/information available with itself or with external reliable sources for the purpose of establishing the identity of the customer. In such cases, a KYC report in a specified format shall be prepared and approved by an appropriate senior official, as may be specified in the KYC/AML procedures. The KYC report shall be stored properly along with other KYC documents.

- Customer specific documentation requirements and other information that is required to be collected would be spelt out separately in the KYC/AML procedures. These documentation requirements and other information requirements shall be reviewed from time to time and would also take into

account the requirements of the various laws/regulations including the Prevention of Money Laundering Act, 2002 as well as extant RBI guidelines

Account opened/operated on behalf of another person/entity

There could be occasions when an account is operated by a mandate holder or in a fiduciary capacity. Under such circumstances, appropriate procedures will be followed.