CHAPTER 4

ANTI-MONEY LAUNDERING ON BANKS

*By K.K. Jindal**

INTRODUCTION

Across the World, banks have become a major target of Money Laundering operations and financial crimes because banks provide a variety of services and instruments that can be used to conceal the source of money. Two cardinal rules that are to be invariably observed by banks for steering clear of the money laundering traps are

1. Know your customer [KYC] and
2. Know your employees

Commercial Banks in India are required to adhere to Anti money laundering guidelines based upon 'Know Your Customer' norms issued by Reserve Bank of India in August- 2002. Banks have been advised to follow customer identification procedure for opening of accounts and monitoring transactions of suspicious nature for the purpose of reporting it to appropriate authority. These 'Know Your Customer' guidelines have been revisited 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 both by the banks/financial institutions in the country has become necessary for international financial relationships. Detailed guidelines based on the Recommendations of the FATF and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision, with indicative suggestions of RBI are discussed in this Chapter.

---

* Programme Director, NIBSCOM, Noida, UP.

Banks have also been advised by Reserve Bank of India to 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 their respective Boards so that banks are fully compliant with the provisions before December 31, 2005. Banks have already taken steps in this direction so as to avoid money laundering related frauds.

The following are the key elements now being observed by banks to curb money laundering

1. Customer Acceptance Policy
2. Customer Identification Procedure
3. Monitoring of Transactions; and
4. Risk Management

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 are required to 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 settlers 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 individual as a 'front' for maintaining accounts with banks. Banks should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

Client accounts opened by professional intermediaries

When the bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Banks may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the bank, the bank should still look through to the beneficial owners. Where the banks rely on the 'customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It should be understood that the ultimate responsibility for knowing the customer lies with the bank.

Accounts of Politically Exposed Persons (PEPs) resident outside India

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

Accounts of non-face-to-face customers

With the introduction of telephone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the

customer to visit the bank branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedure, there must be specific and adequate procedure 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, identify 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.

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 he 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 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 - Name 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 - Name 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, settlers, 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

Banks were advised to put in place a policy framework within three months of the date of the circular and ensure that the banks were fully compliant with the provisions of the Anti money laundering by December 31, 2005. The Chairmen/CEOs of banks were advised by RBI to personally monitor the progress in this regard and take appropriate steps to ensure that systems and procedures were put in place and instructions had percolated to the operational levels. It should also be ensured that there is a proper system of fixing accountability for serious lapses and intentional circumvention of the prescribed procedures and guidelines.

Banks have appointed Principal officers in their banks and put in place a system of internal reporting of suspicious transactions and cash transactions of Rs. 10 lakh and above. In this connection, the Government of India, Ministry of Finance, Department of Revenue, issued a notification dated July 1, 2005 in the Gazette of India, Notify the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts following obligations on the banking companies in regard to preservation and reporting of customer account information.

Maintenance of records of transactions

Banks to have a system of maintaining proper record of transactions as mentioned below:

(i) all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
(ii) all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh;
(iii) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
(iv) all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

Information to be preserved

Banks are required to maintain the following information in respect of specified transactions

(i) the nature of the transactions;
(ii) the amount of the transaction and the currency in which it was denominated;
(iii) the date on which the transaction was conducted; and
(iv) the parties to the transaction.

Maintenance and Preservation of records

Banks are to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requests by the competent authorities. Further, banks are to maintain for at least ten years from the date of cessation of transaction between the bank and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

Records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least ten years after the business relationship is ended. The identification records and transaction data should be made available by Banks to the competent authorities upon request.

Reporting to Financial Intelligence Unit-India

Banks are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

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

Reporting Formats

There are altogether five reporting formats viz.

(i) Manual reporting of cash transactions
(ii) Manual reporting of suspicious transactions
(iii) Consolidated reporting of cash transactions by Principal Officer of the bank
(iv) Electronic data structure for cash transaction reporting and
(v) Electronic data structure for suspicious transaction reporting.
(vi) The reporting formats contain detailed guidelines on the compilation and manner/procedure of submission of the reports to FIU-IND. Banks to initiate urgent steps to ensure electronic filing of cash transaction report (CTR) as early as possible. The related hardware and technical requirement for preparing reports in an electronic format, the related date files and data structures thereof are furnished in the instructions part of the concerned formats. However, banks which are not in a position to immediately file electronic reports may file manual reports to FIU-IND. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, banks have to adhere to the following:
    (a) The cash transaction report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month. While filing CTR, individual transactions below rupees fifty thousand may not be included;
    (b) The Suspicious Transaction Report (STR) should be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer

should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report should be made available to the competent authorities on request;

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

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

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

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

Banks may not put any restrictions on operations in the accounts where an STR has been made. However, banks to ensure that there is no tipping off to the customer at any level.

Conclusion

Money laundering is a serious, highly sophisticated and global criminal activity. The degree of organization displayed in Money Laundering is a major cause of concern for banks and Reserve Bank of India. Banks and Financial Institutions can protect themselves against Money Laundering by implementing an effective KYC policy knowing their customers, checking the source of funds, monitoring the conduct of accounts, and by learning to recognize suspicious/irregular transactions.