

***Know Your Customer (KYC) Norms
And
Anti-Money Laundering (AML) Standards***

GUIDANCE NOTES FOR BANKS

July 2009



Indian Banks' Association



KYC & AML Guidance Notes For Banks

First Edition - October 2005

Second Edition - July 2009



F O R E W O R D

Indian Banks' Association brought out the first edition of "Know Your Customer (KYC) Standards and Anti-Money Laundering (AML) Measures - IBA Guidance Notes for Banks" in October 2005. This was meant to give broad outlines of policy frame work based on international practices to serve as a reference guide to banks in complying with the provisions of the Reserve Bank of India guidelines on "Know Your Customer Guidelines and Anti-Money Laundering Standards" and also to meet the obligations of banks under the Prevention of Money Laundering Act (PMLA) 2002. The IBA Guidance Notes were seen as useful in ensuring uniformity of approach among the banks in implementing the KYC Norms and AML Standards.

Since 2005, there has been a number of developments in AML / CFT regimes globally and in our country and also the RBI has revisited some aspects of their KYC guidelines issued in November 2004. It was therefore felt necessary to review and revise the Guidance Notes by incorporating new developments to serve as a reference document to the banks on all KYC / AML / CFT issues.

The task of revising the Guidance Notes was assigned to a Working Group formed with Senior Executives of member banks overseeing KYC / AML measures. The hard work of going through relevant rules, regulations and guidelines both national and international and redrafting the document was taken up by a Core Group of members drawn from State Bank of India, ICICI Bank Ltd., Standard Chartered Bank and HSBC. The Core Group met on a number of occasions and deliberated on minute details to be incorporated in the draft document before presenting to the Working Group. I understand that the contents of the guidance notes were shared with Reserve Bank of India and Financial Intelligence Unit-India (FIU-IND), New Delhi and their informal but valuable suggestions incorporated in the document. Financial Intelligence Unit - India (FIU-IND) had complimented the efforts made by IBA for preparing comprehensive Guidance Notes for the Industry. FIU-IND also mentioned that the document would be found useful by banks and their employees and improve compliance to the Prevention of Money Laundering Act (PMLA) 2002.



I am sure that the Guidance Notes will create awareness on the legal and regulatory framework for AML / CFT requirements and systems across the banking sector. It would help banks to interpret the obligations under the PMLA and other relevant regulations and how they might be implemented in practice. Also, it would facilitate banks to align their operations with good international industry practices in AML / CFT procedures through an appropriate risk based approach and provide a framework for banks to design and implement the systems and controls necessary to mitigate the risks of the bank being used in connection with money laundering and terrorist financing.

I compliment and place on record my sincere appreciation of the contribution made by members of the Core Group as well as Working Group and IBA secretariat in revising and updating these Guidance Notes.

Mumbai
July 30, 2009

M. V. NAIR

Chairman

INDIAN BANKS' ASSOCIATION



IBA Working Group on KYC & AML

CONVENER

Mr. K Unnikrishnan
Deputy Chief Executive
Indian Banks' Association

MEMBERS

- | | |
|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 1) Mr. B S Bhasin
Chief General Manager (BO)
State Bank of India | 2) Dr. Sanjay Chougule
Global Head - Financial Crime
Prevention & Reputation Risk
Management,
ICICI Bank Ltd. |
| 3) Ms. Neeta Rege
Head, Compliance - Consumer
Banking & CMLPO, India
Standard Chartered Bank | 4) Mr. Robby Abraham
Sr. Vice President - Compliance
HSBC Ltd. |
| 5) Mr. V Ganesan
General Manager
Indian Bank | 6) Mr. K C Pillai
Asst. General Manager &
Principal Officer - AML Cell
Union Bank of India |
| 7) Mr. Manoj Nadkarni
Sr. Vice President
Audit & Compliance
HDFC Bank Ltd. | 8) Ms. Bhuvana Rao
Sr. Vice President
Country AML Compliance
Citibank N.A. |
| 9) Mr. S. Gopal
Chief Manager - AML Cell
Bank of India | 10) Mr. Govind Shukla
Chief Manager
Punjab National Bank |

IBA SECRETARIAT

Mr. Tushar A Shah
Manager



IBA Core Group on KYC & AML

CONVENER

Mr. K Unnikrishnan

Deputy Chief Executive
Indian Banks' Association

MEMBERS

- | | |
|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 1) Mr. B S Bhasin
Chief General Manager (BO)
State Bank of India | 2) Dr. Sanjay Chougule
Global Head – Financial Crime
Prevention & Reputation Risk
Management,
ICICI Bank Ltd. |
| 3) Ms. Neeta Rege
Head, Compliance–Consumer
Banking & CMLPO, India
Standard Chartered Bank | 4) Mr. Robby Abraham
Sr. Vice President - Compliance
HSBC Ltd. |
| 5) Ms. Madhu Sinha
Dy. General Manager
& Head AML
Central Compliance Group
ICICI Bank Ltd. | 6) Mr. K T Mathew
Head - Financial Crime Risk
Compliance & Assurance
Standard Chartered Bank |
| 7) Mr. Arun Boyina
Vice President – Compliance
HSBC Ltd. | 8) Mr. Krishna M Trivedi
Dy. General Manager
State Bank of India |
| 9) Ms. Manisha Agaskar
Head–Transaction Monitoring Unit
Standard Chartered Bank | 10) Mr. Umesh Chandra
Asst. General Manager
State Bank of India |
| 11) Mr. Praveen Mohan Dayal
Chief Manager
ICICI Bank Ltd. | 12) Mr. Narasinh Prabhu
Chief Manager
ICICI Bank Ltd. |

IBA SECRETARIAT

Mr. Tushar A Shah
Manager



Contents	Page No.
<u>PREFACE</u>	
* Preamble	1
* Purpose	2
* Scope	2
<u>CHAPTERS</u>	
1. Overview and Regulatory Frame Work	3
2. Internal Controls and Structure in Banks	13
3. Customer Risk Categorization (CRC)	19
4. Know Your Customer (KYC)	23
5. Reporting Obligation under PMLA Act	34
6. Transaction Monitoring	38
7. Name Screening Process	46
8. Wire Transfers – FATF SR VII Compliance	54
9. Staff and Customer Awareness	57
10. Preservation of Records	60



Contents	Page No.
A N N E X U R E S	
I. Resident Individual Account Opening Form - Annexure A	62
II. Non-Resident Individual Account Opening Form - Annexure B	68
III. Customer Behavior Indicators - Annexure C	75
IV. An Indicative List of Suspicious Activities - Annexure D	76
V. Anti-Money Laundering - Case Studies of Suspicious Activities (Useful For Training Purposes) - Annexure E	85
VI. Suggested solutions to certain situations - Annexure F	115
VII. Reserve Bank of India (RBI) Master Circular dated July 1, 2009 - Annexure G	121



P R E F A C E

Preamble

In India, there had been laws and regulations for quite some time to address certain aspects of money laundering prevention, like Criminal Law Amendment Ordinance 1944 for attachment of proceeds of certain crimes or Reserve Bank of India (RBI) instructions regarding identification requirements for opening of the bank accounts. However, a consolidated anti-money laundering specific legislation, Prevention of Money Laundering Act, 2002 (PMLA), came in to effect with the Government of India Gazette notification on 1st July 2005. The Financial Intelligence Unit-India (FIU-IND) constituted by Government of India on 18th November 2004 as a nodal agency for the anti-money laundering measures also got statutory recognition on 1st July 2005.

In October, 2005 Indian Banks' Association (IBA) issued the "Know Your Customer (KYC) Standards and Anti-Money Laundering (AML) - Guidance Notes for Banks", basically for giving broad outlines of policy frame work based on international practices to serve as a reference guide to the banks in complying with the provisions of the RBI Circular dated 29th November 2004 on "Know Your Customer (KYC) Guidance - Anti-Money Laundering Standards" and also to meet the obligations of banks under the PMLA. The Guidance Notes helped in ensuring uniformity of approach among the banks in implementing the KYC Standards and AML measures.

Since 2005, there has been a number of developments in the Anti-Money Laundering (AML) / Combating of Financing of Terrorism (CFT) internationally and within India that it was considered necessary to review and revise the Guidance Note to incorporate the new developments and to give a more detailed Note that could serve as a reference document to the banks on all KYC / AML / CFT.



Purpose

The purpose of this Guidance Notes is to:

- Create awareness to the legal and regulatory frame work for AML/CFT requirements and systems across the banking sector,
- Interpret the obligations under the PMLA and other relevant regulations and how they may be implemented in practice,
- Help banks to align their operations with good international industry practice in AML/CFT procedures through a proportionate risk based approach, and
- Provide a framework for banks to design and implement the systems and controls necessary to mitigate the risks of the bank being used in connection with money laundering and terrorist financing.

Scope

The scope of these Guidance Notes covers all member banks of IBA. Although these Guidance Notes are designed primarily to cover the activities of banks, the contents are generally applicable to other financial institutions and intermediaries covered under the PMLA and are required to adopt KYC Standards.

It should be noted that these Guidance Notes issued by IBA are voluntary and recommendatory in nature. Failure to comply with these Guidance Notes does not mean that a Bank has automatically breached the Rules under PMLA or any of the Guidelines issued by RBI. They do, however, provide an indication of what the supervisors/ regulators may take into account as being expected of banks. When tailored by a bank to its own risk management architecture and business processes, these Guidelines provide a safety net in respect of Rules and Regulations pertaining to AML.

It may please be noted that these Guidance Notes is an IBA document and the information contained therein is only for the guidance of the industry and ease of understanding of the legal provisions, and for legal purposes the provisions contained in the PMLA and rules there under and instructions issued by RBI from time to time would be applicable.



Chapter 1

OVERVIEW AND REGULATORY FRAME WORK

1.1 What is Money Laundering?

As per the Prevention of Money Laundering Act 2002, the offence of Money Laundering is defined as:

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.

"proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property.

Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of the criminal funds. The proceeds of crime laundered by criminals often are generated in very heinous crimes like drug trafficking, trafficking in women and children, child pornography, extortion, murder, etc.

Money Laundering Prevention, therefore, is not only a statutory or regulatory requirement but also a moral responsibility for all the bank employees as any facilitation of money laundering indirectly supports these criminal activities.

1.2 Terrorist Financing

Terrorists use similar methods as Money Launderers for moving their funds. Some of the terrorist groups also indulge in criminal activities for generating funds for their activities and some of them are even known to have strong relationships with criminal gangs. The two major differences between terrorist financing and money laundering are:

- Terrorist funding can happen from legitimately obtained income whereas the source of money in money laundering is always from illegal source, and



- More often terrorist activities require small amounts and hence it is increasingly difficult to identify terrorist funding transactions.

1.3 Other Financial Crimes

Other financial crimes such as Fraud and market abuse (insider trading) are closely related to money laundering and terrorist financing and most often the measures described in these guidelines for preventing money laundering and terrorist financing may help financial institutions in preventing fraud and other financial crimes, as well.

1.4 International Developments & Recommended Standards

1.4.1 Financial Action Task Force (FATF)

One of the most important events to influence international money laundering prevention efforts was the establishment of FATF by the G-7 Summit in 1989 consisting of the G-7 member states, the European Union and 8 other countries. In April 1990, they came out with the Forty Recommendations that provided a comprehensive plan of action to fight against money laundering. In 2001, the development of standards in the fight against terrorist financing was added to the mission of FATF and it came out with the Nine Special Recommendations for combating terrorist financing. These 40+9 recommendations form the backbone for all the international AML/CFT policies, procedures and processes.

Over the years more members were admitted to the FATF and the current membership is 34, including 32 member states and 2 regional organizations, European Union and Gulf Development Council. India and Republic of Korea are currently countries with observer status aspiring to be full members.

Forty Recommendations

(http://www.fatfgafi.org/document/280,3343,en_32250379_32236930_33658140_1_1_1_1,00.html)

While most of the recommendations are meant for the countries to establish an AML Infrastructure by criminalizing money laundering, making provisions for confiscating assets of the money launderers, establishing Financial Intelligence Unit, transparency of legal persons and arrangements, international co-operation, mutual legal assistance and extradition, etc. the following recommendations relate to measures to be taken by financial



institutions and non-financial entities and professions to prevent money laundering and terrorist financing:

- **Customer due diligence and record keeping**
(Recommendations: 4 to 12)
- **Reporting of suspicious transactions**
(Recommendations 13 to 16)
- **Other measures to deter money laundering and terrorist financing**
(Recommendations 17 to 20)
- **Measures to be taken with respect to countries that do not or in-sufficiently comply with the FATF Recommendations**
(Recommendations 21 and 22)
- **Regulation and supervision**
(Recommendations 23 to 25)

Nine Special Recommendations

(http://www.fatf-gafi.org/document/9/0,3343,en_32250379_32236920_34032073_1_1_1_1,00.html)

These nine recommendations are special measures to combat terrorist financing and include measures to be taken by countries to criminalise terrorist financing, ratification and implementation of UN resolutions on terrorism, freezing and confiscation of terrorist assets, etc. One of the important recommendations concerning banks is Recommendation 7 dealing with "Wire Transfers" which is reproduced below:

Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.

Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers, which do not contain complete originator information (name, address and account number).

FATF also issued an Interpretative Note to Special Recommendation VII :



Wire Transfers. (<http://www.fatf.org/dataoecd/34/56/35002635.pdf>)

Guidance on the Risk Based Approach to Combating Money Laundering and Terrorist Financing

(<http://www.fatf.org/dataoecd/43/46/38960576.pdf>)

This guidelines on the high level principles and procedures in risk based approach in combating money laundering and terrorist financing was prepared by FATF in close consultation with representatives of the international banking and securities sector and was adopted by FATF at its Plenary in June, 2007.

1.4.2 UN Security Council Resolutions 1267 (1999), 1373 (2001) and 1390 (2002)

These UN Security Council Resolutions require members to take steps in preventing terrorism and UN issues lists of names of persons and organizations concerned with terrorism and the member countries are required to freeze their assets.

1.4.3 Wolfs berg Principles - Private Banking & Correspondent Banking

(<http://www.wolfsberg-principles.com/privat-banking.html>) and (<http://www.wolfsberg-principles.com/corresp-banking.html>)

The Wolfs berg Group consisting of 12 leading international financial institutions formulated AML Principles, specially intended for combating increased money laundering risk in case of private banking and correspondent banking. These principles are considered as the most acceptable standards in these areas by most of the major international regulators and institutions.

1.4.4 Asia Pacific Group on money laundering (APG)

Asia Pacific Group on money laundering (APG) has been constituted to facilitate the adoption, implementation and enforcement of internationally accepted standards (such as those issued by FATF) against money laundering and the financing of terrorism. APG also assists its member jurisdictions to enact laws criminalising the laundering of the proceeds of crime and dealing also with mutual legal assistance, confiscation, forfeiture and extradition. APG also guides the member jurisdictions in setting up systems for reporting and investigating suspicious transactions and helps

them in the establishment of financial intelligence units. Presently there are 28 member jurisdictions in APG. Mutual evaluations are the primary means by which the APG monitors progress. Mutual evaluation is a mechanism of multilateral monitoring and peer review of the progress made by members in implementing the FATF Forty Recommendations. The process is designed to identify weaknesses in member jurisdictions and make appropriate recommendations with a view to improvement where they are not.

India was evaluated for its compliance on AML/CFT with 40+9 FATF recommendations by APG in 2005. Following were the recommendations and Comments of the APG in its Mutual Evaluation Report (APGMR) 2005 in regard to FATF recommendation 21 about dealing with countries with insufficient FATF standards:

- Implement measures to require financial institutions to examine the background to transactions that are complex, unusual or have no apparent economic or lawful purpose, and to retain a written record of the examination in line with the underlying transaction record.
- Provide that financial institutions should pay special attention in relation to transactions and relationships that involve persons from or in countries that do not adequately apply the FATF Recommendations.
- Introduce a mechanism to alert financial institutions to those countries that are considered not to apply the FATF Recommendations adequately.
- Introduce an inter-agency procedure for determining whether specific counter measures should be taken, in particular circumstances, against countries that do not adequately apply the FATF Recommendations.

1.5 Legislation & Regulations in India

Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), Insurance Regulatory and Development Authority (IRDA) and FIU-IND are the bodies mainly responsible for the anti-money laundering efforts for financial institutions in India. RBI as the lead regulator for banks and other financial institutions issue regulations on the subject. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister of India and is responsible for



receiving, processing, analyzing and disseminating information relating to suspicious financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and related crimes. The key legislations and regulations towards AML efforts in India are given below:

1.5.1 A) Prevention of Money Laundering Act, (PMLA) 2002

The first step in the anti-money laundering legislation in India was the introduction of the Prevention of Money Laundering Bill 1998 in the Parliament in August 1998. Since the Lok Sabha was dissolved in April 1999, this bill could not be passed. Prevention of Money Laundering Bill 1999 was introduced in the Parliament in October 1999. This bill was passed by the Parliament in 2002 and received President's assent in January 2003 and PMLA, 2002 was enacted. This law came to effect on 01 July 2005 after an amendment.

The act criminalises money laundering and also provides for freezing and confiscation of assets concerned in money laundering. Appointment of various authorities including Financial Intelligence Unit is also covered in its provisions. The Act also lays down obligations of banks in maintaining records of certain prescribed transactions and reporting such transactions to FIU-IND. This also lists out the prescriptive offences, which will come under the purview of the Act.

B) Prevention of Money Laundering (Amendment) Act, (PMLA) 2009

Prevention of Money Laundering (Amendment) Act 2009 was duly notified in March 2009. The key amendments are listed as under:

- The Act incorporates additional categories of offenses punishable under PMLA.
- The Act extends coverage to additional categories of reporting entities such as money remittance businesses/intermediaries, casinos & dealers in foreign currency authorised under FEMA. The Act also provides authority to the Government to extend coverage to other entities.
- Separate categories of offenses with cross border implications have been defined.



1.5.2 Know Your Customer (KYC) Guidelines -Anti Money Laundering (AML) Standards - RBI Circular dated November 29, 2004

This was the major step in the banking industry in India towards money laundering prevention. Though RBI had historically issued guidelines to banks for conducting due diligence of customers including taking photographs, this was the first comprehensive anti-money laundering initiative by RBI. The Guidelines required the banks in India to follow the following steps towards preventing money laundering :

- Customer Acceptance Policy
- Customer identification Procedures
- Monitoring of Transactions, and
- Risk Management

1.5.3 Know Your Customer (KYC) Guidelines - Anti-Money Laundering (AML) Standards - RBI Circular dated August 23, 2005

By this circular RBI has instructed the Banks to apply limited due diligence to people belonging to low income group who are unable to produce CDD documents as prescribed in RBI's KYC Guidelines for opening the accounts. Limits are prescribed for aggregate credits and balance in these accounts.

1.5.4 Anti-Money Laundering (AML) Guidelines for Authorised Money Changers - RBI Circular dated December 2, 2005

These are specific guidelines issued by RBI for authorised moneychangers for complying with the requirements of PMLA. They are required to do due diligence on their customers, depending on the value of the transactions. They are also required to maintain records of certain prescriptive transactions and report suspicious activities to FIU-IND. This circular also puts restrictions on cash transactions for both purchase and sale of foreign currency.

1.5.5 Guidelines for Anti-Money Laundering (AML) Measures issued by SEBI dated January 2006

SEBI issued these guidelines to all the SEBI regulated entities for complying with the requirements of PMLA, like CDD on customers, maintaining records of prescriptive transactions, reporting of suspicious activities, etc.



1.5.6 Prevention of Money Laundering Act, (PMLA) 2002 - Obligation of Banks in Terms of Rules Notified there under - RBI Circular dated February 15, 2006

Consequent to the PMLA 2002 coming into effect and notification of the rules framed there under, RBI issued this circular to issue detailed instructions regarding the responsibilities of the regulated entities under the act, especially on the following points :

- Appointment of Principal Officers
- Reporting of cash transactions above INR 1 million
- Reporting of integrally connected cash transactions below INR 1 million but the aggregate amount exceeded INR 1 million within a period of one month.
- Reporting of counterfeit currency notes and forged valuable securities detected, and
- Reporting of all suspicious transactions

1.5.7 Know Your Customer (KYC) Norms/Anti Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT) - Wire Transfers - RBI Circular dated April 13, 2007

RBI vide this circular has given specific instructions regarding furnishing of originators name and address/ account details in the cross border and domestic wire transfers.

1.5.8 Know Your Customer (KYC) Norms/Anti-Money Laundering (AML) Standards /Combating of Financing of Terrorism (CFT) - RBI Circular dated February 18, 2008

This circular clarifies certain points regarding CDD documentation as required in the KYC Guidelines and AML Standards and also on risk categorization review of accounts, periodic KYC updation and screening of names against lists of entities contained in the UN Security Council resolutions in their anti money laundering and terrorist financing measures.

1.5.9 Prevention of Money Laundering Act, (PMLA) 2002 - Obligation of banks in terms of Rules notified there under - RBI Circular dated May 22, 2008

This circular clarifies on the reporting obligations under the PMLA, especially on what constitute integrally connected cash transactions and also on reporting requirements irrespective of the threshold applicable for certain



prescriptive offences in the PMLA.

1.5.10 Know Your Customer (KYC) Norms/Anti-Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act, (PMLA) 2002 - RBI Master Circular dated July 1, 2009

This latest master circular issued by RBI consolidates all the instructions issued in the earlier circulars on KYC norms, AML standards, CFT and obligations of banks on PMLA. RBI had started issuing master circulars on KYC/AML/CFT on annual basis from July 2008.

1.5.11 UN Security Council Resolutions 1267 (1999) - RBI Circulars

RBI periodically issues circulars following on UN Security council resolutions on measures taken by the UN for money laundering prevention and combating terrorist financing. The names of the persons/ entities contained in these circulars are required to be maintained as a watch list to prevent accounts being opened in these names or transactions being done with them as counter parties. The updated list of such persons and entities can be accessed at the UN site <http://www.un.org/sc/committees/1267/consolist.shtml>.

1.5.12 UN Security Council Resolutions on Iran - RBI Circulars dated September 10, 2007 and September 19, 2008

These circulars were issued in pursuance of UN Security Council Resolutions 1737/2006 and 1803/2008 on Iran. Banks have been advised to check for accounts and transactions involving the listed entities and persons and to report to RBI and FIU-IND any accounts held in these names. Banks were also advised to exercise vigilance over the activities of financial institutions and banks domiciled in Iran, in particular, with bank Meli and Bank Saderat and their branches and subsidiaries abroad, in order to avoid such activities contributing to the proliferation sensitive nuclear activities or to the developments of nuclear weapon delivery systems as referred to in UNSCR 1737/2006.

1.5.13 FATF's statement highlighting deficiencies in the AML/CFT systems in certain jurisdictions - RBI Circular dated February 2, 2009 - This has been reiterated by RBI in its Master Circular dated July 1, 2009

The RBI circular, quoting the statements issued at the Plenary of FATF held on February 28, 2008 and October 16, 2008, advises banks and financial institutions to take into account risks arising from the deficiencies



in the AML/CFT regime of six countries namely Sao Tome and Principe, Turkmenistan, Iran, Northern Part of Uzbekistan and Pakistan.

Accordingly, banks and financial institutions may place these countries in a higher risk category, and put in place a framework to monitor the cross border transactions involving these countries.

1.6 Extra-territorial Applicability of the Indian Anti-Money Laundering Laws and Regulations

As per the provisions of PMLA, Central Government of India may enter in to reciprocator agreement with other countries for implementation of all or some of the provisions of the Act in that country.

The RBI regulations are applicable to all the branches of subsidiaries of Indian banks functioning in other countries and for these institutions where the host country regulations are more onerous; the host country regulation will prevail.

1.7 Implications of International Regulations - UN / US / EU Sanctions

International bodies such as the United Nations (UN) and other regulators belonging to the United States (US) and European Union (EU) periodically release information on the various sanction programmes imposed at country and individual / entity level with regards to AML/ CFT measures. Member nations of the UN need to comply with the resolutions passed at the UN. Banks are advised by RBI for complying with the same.

Where the Bank has a US listing, or has activities in, or linked to, the USA, whether through a branch, subsidiary, associated company or correspondent bank relationship, there could be application of US AML/ CTF and financial sanctions regimes to the non-US activities of the firm, e.g. US Dollar transactions cleared through US. It essentially means that though a particular US AML / CTF or financial sanction may not be applicable directly to a transaction if done in India, it may become applicable if it is carried out in US dollar or any 'US person' like a US based bank or branch is involved in the transaction. Banks may take appropriate advice on the extent to which the firm's activities may be covered in this way.

Similarly, for transactions denominated in Euros or routed through European Banks, the sanctions imposed by EU would be applicable.

Banks in India need to be aware and create a framework for complying with these sanction programmes to the extent applicable.



Chapter 2

INTERNAL CONTROLS AND STRUCTURE IN BANKS

2.1 What are the roles and responsibilities of Board of Directors and Senior Management

The Board of Directors and the senior management of the bank have the responsibility to ensure that the bank's control processes and procedures are appropriately designed and implemented, and are effectively operated to reduce the risk of the Bank being used in connection with money laundering or terrorist financing.

Appointment of Principal Officer

It is the responsibility of the Board of Directors to appoint the Principal Officer (PO). It is recommended that the PO has a sufficient level of seniority within the bank and has sufficient resources, including sufficient time and (if necessary) support staff. The level of resources should reflect the size, complexity and geographical spread of the bank's customer/product base and should include arrangements to apply in the event of the temporary absence of the PO.

2.1.1 Managing the risk of money laundering

The senior management of the bank is required to ensure that appropriate risk-based policies are in place across different aspects of the business. The banks should adopt an approach to mitigate themselves of the risk of being used for the purposes of money laundering or terrorist financing. Senior management must be entirely engaged in the decision-making and must take ownership of the risk-based approach, since they will be held accountable if the approach is inadequate.

2.1.2 Formulation of appropriate procedures to prevent money laundering

As per the RBI master circular dated July 1, 2009, banks are required to formulate appropriate procedures to prevent money laundering, specifically:

- a. KYC policies and procedures specifying the objective of KYC framework, i.e. appropriate customer identification. The KYC policies should incorporate the following four key elements:
 - Customer Acceptance Policy;



- Customer Identification Procedures;
 - Monitoring of Transactions; and
 - Risk management
- b. Monitor transactions of a suspicious nature;
 - c. Risk management and monitoring procedures, i.e. staff awareness, identification and reporting of suspicious transactions, record keeping of transactions;
 - d. Treating the information collected from the customer for the purpose of opening of account as confidential and not divulge any details thereof for cross selling or any other purposes;
 - e. Ensuring that any remittance of funds by way of demand draft, mail/ telegraphic transfer or any other mode and issue of travelers' cheques for value of INR 50,000 and above is effected by debit to the customer's account or against cheques and not against cash payment;
 - f. Ensuring that the provisions of Foreign Contribution and Regulation Act, 1976 wherever applicable, are adhered to strictly.

Guidance against "Tipping off"

Senior management should provide sufficient guidance to staff to ensure that the customers are not informed (i.e. tipped off) that his/her accounts are under monitoring for suspicious activities and/or that a disclosure has been made to the FIU-IND.

The Bank can however make normal enquiries to learn more about the transaction or instruction to determine whether the activities of the customer arouse suspicion.

Where it is known or suspected that a STR has already been made internally or externally, and it then becomes necessary to make further enquiries, care must be taken to ensure that the suspicion is not disclosed either to the client or to any other third party. Subject to internal procedures, such enquiries should normally/only be made as directed by the Principal Officer (PO).

Internal Reporting Procedures

Reporting lines should be as short as possible, with the minimum number



of people between the person with the suspicion and the PO. This ensures speed, confidentiality and accessibility to the PO. All procedures should be documented in an appropriate manual or handbook and job descriptions drawn up. All suspicions reported to the PO should be documented (in urgent cases this may follow an initial discussion by telephone).

All internal enquiries made in relation to the report, and the reason behind whether or not to submit the report to the FIU-IND, should be documented. This information may be required to supplement the initial report or as evidence of good practice and best endeavors if, at some future date, there is an investigation and the suspicions are confirmed.

2.2 What are the roles and responsibilities of the staff

2.2.1 Keeping abreast with AML information relevant to their role

The communication of a Bank's policies and procedures to its staff to prevent money laundering, and the training in how to apply those procedures, is the key to the success of anti-money laundering strategies. The staff that are interacting with customers or handling customer transactions/instructions will be a Bank's strongest defense against money laundering or its weakest link. The means by which their obligations are communicated to them, and the effectiveness of the associated training, will therefore determine the success of the bank's anti-money laundering efforts. Therefore, as much as it is important for the Bank to communicate the policies and procedures to its staff, it is equally important for the staff to keep themselves abreast with the policies and procedures relevant to their role.

2.2.2 Reporting of suspicious transactions

Every employee has an obligation to report transactions suspicious of a money laundering or terrorist financing activity. It is required to report suspicious transactions even if the employee does not know precisely what the underlying criminal activity is or whether illegal activities have occurred.

The reporting system is suspicion based as opposed to transactions or value based. A suspicion is what it means to the person who decides to report. It is a wholly subjective and analytical concept. The golden rule is, even after undertaking the due diligence, if there is still a doubt, report.

The reporting of these transactions by an employee does not constitute



a breach of the employee's duty of confidentiality owed to customers. In addition, as per the PMLA 2002, the banks and their officers shall not be liable to any civil proceedings against them for furnishing information on any suspicious transaction.

2.3 What are the roles and responsibilities of the Principal Officer

Banks must take reasonable steps to give its PO, or any person to whom the PO's duties have been delegated, access to any information it has about the customer or transaction(s). The PO will support and co-ordinate senior management focus on managing the money laundering/terrorist financing risk in individual functions within the bank. The bank should make the PO responsible for the following:

2.3.1 Reporting Requirements

Ensuring that the reporting obligations under PMLA are met, i.e. furnishing FIU-IND information relating to:

- i. All cash transactions of the value of more than INR 1,000,000 or its equivalent in foreign currency;
- ii. All series of cash transactions integrally connected to each other which have been valued below INR 1,000,000 or its equivalent in foreign currency where such series of transactions have taken place within a month, however, aggregating to more than INR 1,000,000;
- iii. All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions; and
- iv. All suspicious transactions whether or not made in cash. To this effect, the bank should make PO responsible to receive the internal suspicious activity reports within reasonable period of time so as to meet the reporting deadline to FIU-IND.

In case of banks, where all the branches are not yet fully computerized, the PO of the bank should cull out the transaction details from branches which are not computerized and suitably arrange to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on their website.

The PO should also ensure that any significant issues are reported to the senior management of the bank on a periodic basis.



2.3.2 Review the adequacy of AML systems and controls

Banks are required to carry out regular assessments of the adequacy of its systems and controls to ensure that they manage the money laundering risk effectively. Oversight of the implementation of the bank's AML/CFT policies and procedures, including the operation of the risk-based approach, is the responsibility of the PO, under delegation from senior management. He/she must therefore ensure that appropriate monitoring processes and procedures across the bank are established and maintained.

The PO should also get actively involved in the selection of the appropriate software for monitoring of customer transactions/activities.

2.3.3 Liaison with various stakeholders/parties

The PO should maintain liaison with various stakeholders/parties, such as regulators (internal and external), FIU-IND, IBA and other member banks. Specifically, the PO should ensure that any queries raised by the regulators are answered within the stipulated deadlines.

2.3.4 Staff awareness - provision of relevant information to staff

The PO is responsible for oversight of the bank's compliance with its requirements in respect of staff training, including ensuring that adequate arrangements for awareness and training of employees are in place. Although this is a bank-wide responsibility, there may be some delegation to appropriate persons/functions in business areas. The PO, however, is responsible for ensuring that the training is offered, that the standards and scope of the training are appropriate, and that appropriate records are kept.

To this effect, the bank should also make the PO responsible to keep himself/herself abreast of developments in the AML environment at national and international level. The PO should also disseminate relevant information to the business heads and staff in a timely manner.

2.4 What are the roles and responsibilities of the Internal Audit/Internal Control

The Internal Audit and Internal Control teams within the banks would be responsible to ascertain the effectiveness and efficiency of the AML framework of the bank. This would specifically include checking the adequacy of policies, procedures, and system support to detect suspicious and potential money laundering transactions, and the subsequent monitoring and reporting to regulators, FIU-IND and senior management.



2.5 What are the roles and responsibilities of the Business Groups

Banks may consider appointing business groups, who are usually the heads of the respective businesses/functions within the bank. The responsibilities of the business groups would be as follows:

- a. Assist line management in their responsibility for complying with all relevant AML regulations and standards;
- b. Cascade AML related information and requirements to department staff and to ensure AML related requirements are incorporated into operating procedures;
- c. Monitor adherence to AML procedures and controls. In particular, to monitor changes to business practices and products to ensure that AML procedures and controls are adequate to cover them;
- d. Assist in the provision of anti-money laundering training, where necessary;
- e. Report all material and significant breaches or potential breaches of AML requirements to the PO.



Chapter 3

CUSTOMER RISK CATEGORIZATION (CRC)

3.1 What is Customer Risk: 'Customer risk ' in the present context refers to the money laundering risk associated with a particular customer from a bank's perspective. This risk is based on the risk perceptions associated with the parameters comprising a customer's profile, and the level of risk associated with the product and channels being used by him.

3.2 Need for Customer Risk Categorization: The RBI master circular dated July 01, 2009 on Know Your Customer (KYC) Norms/Anti Money Laundering Standards, which consolidates all guidelines issued on the subject, requires the banks to categorise customers into low, medium, & high risk categories and have differential due diligence and monitoring standards based on the risk assessment.

The guidelines mention some of the parameters, which may be considered for categorising a customer's risk. Examples of some high risk categories are also given, which include Non Resident Indians (NRIs), High Networth Individuals (HNIs), Trusts, Charities, Non Governmental Organisations (NGOs), companies having closed shareholding structure, firms with sleeping partners, Politically Exposed Persons (PEPs), non-face-to-face customers, persons with dubious reputation, etc.

The guidelines further require the banks to carry out a review of risk categorization of customers at a periodicity of not less than once in six months. It is therefore, now mandatory for banks in India to introduce a system of CRC for their customers.

3.3 Risk based approach: RBI guidelines also reiterate that Banks should follow a 'risk based approach' on KYC/AML standards to avoid disproportionate costs and a burdensome regime for the customers. Categorising customers into different risk buckets can serve as a platform to adopt such approach.

3.4 Approach for Customer Risk Categorization: Customers may be classified into low, medium and high risk. Customers requiring higher level of monitoring may if considered necessary be classified even higher.



Each bank may develop its own model for customer risk categorization based on available product/customer information, risk perception, and other factors such as available technology, etc. A profile of the customer may be created in the system using available information based on which the risk should be assigned. The following broad approach may be adopted for risk categorisation:

- A) Selection of Parameters for risk categorization: The first step in process of risk categorization is selection of parameters, which would determine customer risk. Some indicative parameters, which can be used to determine the profile & risk category of a customer, are as follows:
1. Customer constitution: Individual, proprietorship, partner-ship, private limited, etc
 2. Business segment: Retail, Corporate, etc
 3. Country of residence/ Nationality: Whether India or any overseas location/ Indian or foreign national.
 4. Product subscription: Salary account, NRI products, etc.
 5. Economic profile: HNI, public limited company, etc.
 6. Account status: Active, inoperative, dormant.
 7. Account vintage: less than six months old, etc.
 8. Presence in regulatory negative/PEP/defaulters/fraudster lists.
 9. Suspicious Transaction Report (STR) filed for the customer.
 10. AML Alerts

Other parameters like source of funds, occupation, purpose of account opening, nature of business, mode of operation, credit rating, etc can also be used in addition to the above parameters. Banks may adopt all or some of these parameters based on availability of data.

- B) Deciding on type of classification- Banks may choose to carry out either Manual Classification or Automated Classification using technology systems or a combination of both. In case of manual classification each customer would be classified based on the risk parameters and assigned risk on a case to case basis. In case of banks wanting to do a manual CRC, they may adopt suitable parameters from indicative list above and accordingly devise a model/ policy for assigning risk category to each customer/customer segment.



In case of automated classification, the banks computer systems would assign risk based on parameters adopted using standard rules and scale for same.

- C) Determining the Risk rating methodology Once the parameters are finalized, depending upon the data availability banks may choose an appropriate risk rating model. One of the easy to use models is the weighted average method. In the weighted average method each parameter is assigned a 'risk score' and a 'weight' is attached to the parameter depending upon its accuracy and criticality to the overall risk. The output score is compared to a final scale. Banks need to ensure that while assigning risk score and weight to various parameters, Critical and more accurate parameters like customer constitution and product subscription are given their due weightage.
- D) Risk Categories: Depending on the risk score obtained as per the above method, the customers will be assigned low, medium and high risk ratings. Banks may also choose additional categories or sub divide these main categories such as 'very low' or 'very high'.

Note : Loan accounts of non-operative nature having a pre-determined cash flow (e.g. home loans), and fixed cap accounts like the small deposit accounts, can be regarded as low risk.

3.5 Use of Software for risk categorization: Banks may (if required by their approach to risk categorization), deploy suitable software for purpose of risk categorisation. Such software can be used to extract customer data from the banking software and assign risk rating based on the scoring model selected by the bank. If a bank chooses and if its core banking application permits, CRC maybe done in the core banking software as well.

3.6 CRC and Transaction Monitoring: A risk based approach on AML requires the CRC to be linked to transaction monitoring process, with a high risk account requiring a more enhanced monitoring by way of lower thresholds and periodical reviews, as compared to a low risk account.

3.7 Periodic review of CRC: RBI guidelines mandated that a review of risk categorization of customers should be carried out at a periodicity of not less than once in six months. Since CRC is an on going process, a 'risk



date' i.e. a cut-off date would need to be determined to serve as a start date for the process of risk categorisation. The periodic reviews would be calculated from this start date. During such review, the risk assigned to an existing customer may undergo change depending on the change in parameters consisting his profile.

3.8 Risk Categorisation of Existing Customers: The main challenge of CRC for the legacy customers is the availability and accuracy of available data. Banks may therefore need to categorise customers based on available information.

3.9 Conclusion:

- CRC enables a bank to follow a risk based approach on AML/ KYC as per the RBI guidelines.
- The customer risk may be integrated with transaction monitoring by adequately adopting differential rules/ thresholds for different risk profiles.
- Enhanced due diligence/periodic review for high risk customers can be adopted based on CRC.
- The RBI guidelines also mandate a periodic KYC updation of customers based on their risk profiles. CRC will also help in effective implementation of this requirement.



Chapter 4

KNOW YOUR CUSTOMER (KYC)

4.1 Customer defined: The RBI Master Circular dated July 1, 2009 on Know Your Customer (KYC) Norms & Anti Money Laundering Standards, which consolidates all guidelines issued on the subject, defines 'Customer' as:

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

Banks need to frame policies, which will enable the identification of the customer. The KYC policy of a bank should incorporate the following four elements:

- a) Customer Acceptance Policy;
- b) Customer Identification Procedures;
- c) Monitoring of Transactions; and
- d) Risk Management

4.2 Customer Acceptance Policy (CAP): Every bank should develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place on the following aspects of customer relationship in the bank:

- i. No account is opened in anonymous or fictitious / benami name(s);
- ii. The customers are categorized as per their risk perception based on their profile (See Chapter 3 - Customer Risk Categorization)



- iii. Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk. (For details see the note below on Types of CDD)
- iv. Not to open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures. (Please see below for a detailed note on CDD).
- v. Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity.
- vi. Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organisations etc. (See Chapter 7 - Name Screening Process)

4.3 Customer Identification Procedures: The above mentioned master circular requires banks to clearly spell out the Customer Identification Procedure to be carried out at different stages i.e. while establishing a banking relationship; carrying out a financial transaction or when the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data. Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Banks need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship.

4.4 Establishing Identity

It is important to recognise that the customer identification process does not start and end at the point of application. However, the process of confirming and updating identity and address, and the extent of additional KYC information collected, will differ from bank to bank.

What is Identity?

Identity generally means a set of attributes which together uniquely



identify a natural or legal person. The attributes, which help establishing the unique identity of a natural or legal person, are called 'identifiers'. Name (in full), Father' Name, Date of birth, Passport number, Election Card number (EPIC number), PAN number, Driving License number, etc are unique identifiers available which help establishing the identity of a natural or legal person. These are termed as 'primary identifiers' as they help in uniquely establishing the identity of a natural or legal person.

Addresses / location and nationality and other such identifiers may serve as secondary identifiers' as they help further refine the identity though they may not directly help uniquely identify a natural or legal person.

4.5 What is Customer Due Diligence?: *Customer Due Diligence (CDD) can be defined as any measure undertaken by a financial institution to collect and verify information and positively establish the identity of a customer.* The base of CDD would be the board approved Customer Acceptance Policy of a bank. Based on Customer Acceptance Policy, the Customer Identification Procedures needs to be drawn.

4.6 When should a bank apply CDD?: CDD should be conducted as a part of the Customer Identification Procedures. A bank should apply Customer Due Diligence measures when it:

- i. establishes a business relationship;
- ii. carries out an occasional transaction;
- iii. suspects money laundering or terrorist financing; or
- iv. doubts the veracity of documents, data or information previously obtained for the purpose of identification or verification

4.7 When a Bank is unable to apply Customer Due Diligence measures, it:

- i. must not establish a business relationship or carry out an occasional transaction with the customer;
- ii. should not carry out a transaction with or for the customer through a bank account;
- iii. should terminate all existing business relationship with the customer;
- iv. should consider whether it ought to report to FIU-IND/ Regulators, in accordance with extant guidelines.



4.8 Types of CDD: There are three types of CDD that can be used by a bank in accordance with the risk category of the customer. These are listed as follows:

1. **Basic Due Diligence:** This implies collection and verification of identity proof, address proof and photograph to establish the identity of the customer. This is based on documents and forms the basis of the KYC program for a bank. Different set of documents can be listed for different types of customers. A bank can draw reference from the list of indicative documents provided by the above mentioned master circular but should not restrict itself solely to that list. Documents other than the indicative list such as a property tax bill issued by the local authorities as address proof is as acceptable as any other proof. Banks can have their own list of acceptable documents for KYC as long as they can verify the same with the original. It has been observed that some customers find it difficult to produce the address proof in their own name. In such cases, address proof in the name of their close family members along with a relationship proof may also be accepted.
2. **Simplified Due Diligence:** Any due diligence applied to establish the identity of customer, which involves measures less stringent than basic due diligence can be termed as 'Simplified Due Diligence'. As per the above mentioned RBI guidelines, simplified due diligence can be applied to accounts of people belonging to low income group, both in urban as well as rural areas, to enable 'Financial Inclusion' of this segment. It can also be applied to accounts which have a financial cap, like the "Small Deposit Accounts" where the balances of all accounts and total credits of all accounts at any point of time in a year should not exceed Rs. 50,000/- and Rs. 1,00,000/- respectively. Simplified due diligence can also be applied to low value/ non-recurring transactions. For example, relying on third party certification in case of lending through Business Correspondents and Micro Finance Institutions can be taken as a form of simplified due diligence.
3. **Enhanced Due Diligence (EDD):** Any additional due diligence measures undertaken over and above the basic due diligence can be termed as 'Enhanced Due Diligence'. As per the above-mentioned RBI guidelines, EDD needs to be undertaken for all the high-risk customers of a bank.



EDD can also be built in the account opening processes at the product level or customer type level, where the high risk customers are easily identifiable (e.g. NRIs, Trust accounts, Correspondent banking). Other EDD measures like enhanced level of transaction monitoring for high-risk customers can be undertaken for customers who fall in the high-risk category post the exercise of customer risk categorisation. EDD on existing accounts may also be conducted if required when AML alerts are generated as a part of the transaction monitoring process.

4.9 Specific types of relationships where EDD measures could be applied are:

- i. **Politically Exposed Persons (PEPs):** 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. Persons of foreign origin/ diplomatic missions, such as the ones listed above, located in India, also qualify as PEPs. Persons holding prominent positions in multilateral agencies such as the United Nations, World Bank, etc, can also be construed as PEPs. PEPs of foreign origin and their associates and relatives form group of customers, which should be considered as 'High Risk' by the Bank. Bank should obtain additional information/carry out additional due diligence depending on the risk perception in respect of transactions handled on their behalf. Banks should however, take care not to deny service to PEPs on account of their higher risk perception.
- ii. **High Risk Countries:** Customers who live in countries that are considered High Risk or deficient in respect of implementation of KYC and Anti Money Laundering measures should be classified by a bank as high risk. Each Bank should draw its own list of high risk countries for monitoring of such customers. The list can be based on parameters such as FATF membership, advisories issued by FATF/UN on certain countries, etc. A country risk rating can be further integrated into the customer risk emanating from the country of their residence.
- iii. **Specific types of business:** Customers having business where value of the goods is not easily assessable like antique dealers and businesses dealing in money as a commodity like money exchange bureaus need



to classify as high risk.

- iv. **Trust accounts:** Would require strict documentation and due diligence to be exercised as given in the KYC documentation table below. Trusts are popular vehicles for criminals wishing to avoid the identification procedures and mask the origin of the criminal money they wish to launder. The principal objective for money laundering prevention via trusts is to verify the identity of the provider of funds/ those who have control over the funds, i.e. the grantors, settlers & trustees.
- v. **Non resident Indians (NRIs)/Foreign Nationals:** Indian customers resident overseas and foreign nationals based in India pose a bigger risk from money laundering perspective than ones placed domestically.
- vi. **Non face-to-face customers:** Customers with whom the bank has not had direct interaction at the time of opening the account would require stricter documentation as the Bank may specify. e.g. Certification by independent authority such as notary, foreign resident banks, correspondent banking partners, embassy officials; insisting on additional documentation to establish identity and address etc.
- vii. **Correspondent Banking:** Transactions conducted through correspondent relationships need to be managed taking a risk-based approach. "Know Your Correspondent" procedures should be established to ascertain whether the correspondent bank or counterparty is itself regulated for money laundering prevention and, if so, whether the correspondent is required to verify the identity of their customers to FATF standards. Where the correspondent bank are not following FATF guidelines, additional due diligence should be exercised. Additional due diligence will be required to ascertain and assess the correspondent's internal policy on money laundering prevention and its KYC procedures.

Transactions conducted through correspondent relationships need to be monitored taking a risk-based approach. Particular attention should be paid to the type of business that the correspondent engages in, the market place in which it operates, etc. A country risk rating model can be used to evaluate money laundering risk emanating from the country of location & operations.



- vii. **Fiduciary Accounts:** Bank may exercise enhanced due diligence at the time of opening fiduciary accounts by intermediaries such as guardians of estates, executors, administrators, assignees, receivers etc. For e.g. While opening of the account of an administrator of the estate, it may be necessary to examine the Letter of Administration (Authority) as it would give a picture of the assets of the estate.
- viii. **Pooled Accounts** - Pooled Accounts are essentially fiduciary accounts where investments of a number of persons are pooled together. Normally, such accounts are titled to reflect that the account is being held by a fiduciary. The fiduciary or financial intermediary operating the pool is expected to maintain records that contain statements of all accounts giving investments and disbursements. Pooled accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds, etc., may not pose much difficulties as these are generally regulated entities. Banks may also come across pooled accounts managed by lawyers, chartered accountants or stockbrokers on behalf of a range of clients. Banks should endeavor to satisfy about the identity of individual investors/beneficiaries of the pool at the time of opening such account. Banks should also satisfy that the intermediary managing the pool in a fiduciary capacity maintain proper accounts of individual investors.

4.10 In case of high risk customers, banks may obtain additional information on the customer beyond documentary evidence. An indicative list is as under:

- Information on net worth
- Intended business activity in case of NRI customers
- Report by relationship manager/ branch manager
- Higher level of approvals
- Verification of customer information with independent data sources

4.11 Transaction Monitoring: (See Chapter 6 - Transaction Monitoring)

4.12 Risk Management: (See Chapter 2 - Internal Controls and Structure in Banks)



Note: In accordance with the RBI guidelines on outsourcing, KYC compliance for a bank should not be outsourced.

4.13 The practice of obtaining Introduction

The system of obtaining introduction of prospective customer by an existing customer with whom the Bank has had satisfactory dealings is in vogue in the Indian Banking system. Introduction is also a recognized due diligence procedure to obtain protection under sec 131 of NI Act 1881 relating to collection of instruments. Introduction by an existing customer is not mentioned as a procedure for identifying the customer under FATF and RBI guidelines of November 2004. However, with a view to ensure that strict adherence to KYC Standards would not result in basic banking services being denied to underprivileged segments of the society (financial exclusion) the RBI has permitted flexibility in KYC Standards in opening of accounts for such persons vide Circular DBOD.NO.AML.BC.28/14.01.001/2005-06 dated August 23, 2005. Flexibility allowed in such cases provide for obtaining introduction when the prospective customer is unable to furnish the documents given in the guidelines issued by the RBI. Banks currently following this procedure may, at their discretion, continue the same, while complying with the present guidelines.

KYC UPDATION

4.14 Meaning: As defined in the above mentioned RBI guidelines, customer identification means "identifying the customer and verifying his/ her identity by using reliable, independent source documents, data or information". These guidelines require the banks to "introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened". Therefore '*KYC updation*' can be defined as a process of customer identification and consequent re-affirmation of his identity using reliable, independent source documents, data or information available, in addition to the collection of a photograph.

4.15 Need for KYC updation: RBI guidelines require banks in India to "introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. The periodicity of such updation should not be less than once in five years in case of low risk category customers and not less than once in two years in case of high and medium risk categories."



4.16 Basis for KYC updation: Since the KYC updation is to be carried out based on the risk category of the customer; it becomes essential that all customers of the bank have been given a risk category before proceeding for KYC updation.

4.17 Approach for KYC updation: Before developing their own approach for KYC updation, banks need to assess the following:

- I. Results of the risk categorisation exercise.
- II. Availability of KYC data of the customers in electronic database.
- III. Demographic spread of the customers i.e. location of the customer, type, whether rural or urban, etc.
- IV. Past experiences in customer contact

Based on the above assessment, each bank may decide on a suitable method for KYC updation. Some options, which may be adopted, are as under:

- **Customer Contact:** Under this approach, banks would contact all customers directly through various means such as branch walk-ins, letters, e-mails, phone, etc., asking them to furnish their KYC documents afresh. Banks could also use pre-printed standard letter formats to seek customers' confirmation on the KYC records available in their database. Customers confirmations may be obtained by post or through branches. Similar confirmations can also be obtained over other channels like Internet/phone banking/ATMs. As is evident, this method would warrant a large campaign for contacting the customers and may be a challenge in terms of resources and cost.
- **Relationship KYC:** Under this approach, any new account opened by the customer is linked to his existing relationship with the bank. For example, a savings account customer who is more than five years old comes to open a current account. Bank identifies him as an old customer, and looking at his account vintage, he is asked to furnish a fresh KYC. The KYC procedures applied at this stage may be considered as KYC updation. The KYC updation in this case is done at the Customer ID/relationship level.



- **Surrogate methods of KYC updation:** Some of the customer identification data available with the bank may also be verified with independent and authentic public sources and confirmed. For example, a PAN card taken as identity proof at the time of initial KYC can be verified with the PAN number on Income Tax website to confirm its validity and existence of the customer. Company's details can be checked from Ministry of Corporate Affairs (MCA) website. Such verification may be deemed as updation of customer identification data. Other surrogate measures such as delivery of bank statements and deliverables to the customer's address, telephone directory search etc. may be considered as reaffirmation of his address. Collection of scanned images from customers over secured connections or through registered e-mail IDs in lieu of physical copies of the KYC documents may also be used as additional measures for KYC updation.

Banks may adopt one or a combination of the above suggested approaches depending on their business model, customer-base, and available technology, data and resources.

- **Scope of KYC Updation:** Accounts of some publicly known entities like Government departments and listed companies may be excluded from this exercise. Asset products of non-transactional nature like home loans, personal loans, etc. which carry low AML risk and where a higher level of due diligence has been conducted at the time of credit exposure may also not require KYC updation. For asset products like Cash Credit, Overdrafts, and Credit Cards, which are subject to periodic review/renewal, KYC updation may be treated as a part of the review/renewal exercise. Similarly, non-transactional liability products like term deposits and restricted value accounts like the small deposit accounts also can be kept out of the purview of KYC updation due to the low AML risk.

Note : Identity of the customer does not change over the lifetime of the customer. The identity verification needs to be done only to confirm his current existence, and validity of the identity document.

4.18 Other Aspects related to KYC updation:

Software & channel capabilities: Banks would need to determine its software and channel requirement for this exercise. If a bank wants to store scanned

images of the KYC documents for future references, then appropriate systems need to be implemented. In case multiple channels such as branches, phone banking, Internet banking etc. are proposed to be used in the process of updation, integration of channels is essential to avoid duplication and to bring about synergy and uniformity in their effectiveness. For example, KYC updation using branch banking channel is a more direct way of KYC updation than through phone banking. To make the phone call updation as effective, suitable verification parameters should be put in place.

- 4.19 Making customer responsible for KYC updation:** The customer may be informed about his obligation to fulfill the RBI requirements of KYC updation. This can be done by incorporating appropriate clause in the Account Opening Form (AOF), by way of periodic reminders in the communication sent out to him, or through customer education campaigns.



Chapter 5

REPORTING OBLIGATION UNDER PMLA ACT

5.1 In terms of the Rules notified under Prevention of Money Laundering Act, 2002 (PMLA) certain obligations were cast on banking companies with regard to reporting of certain transactions. The RBI has issued circular No DBOD.NO.AML.BC.63 /14.01.001/2005-06 dated February 15, 2006 and DBOD.AML.BC. No. 85/ 14.01.001 / 2007-08 dated May 22, 2008, detailing the obligation of banks in terms of the Rules notified under PMLA.

Accordingly, Banks are required to make the following reports to the FIU-IND.

- Cash Transaction Reporting (CTR)
- Counterfeit Currency Reporting (CCR)
- Suspicious Transaction Reporting (STR)

5.2 Cash Transaction Reporting (CTR)

As per the PMLA rules, Bank is required to submit the details of:

All cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency.

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.

The format for reporting of the above-mentioned cash transactions, known as Cash Transaction Report (CTR) has been provided by the RBI vide its circular dated February 15, 2006. This report is required to be filed on a monthly basis by 15th of the succeeding month.

RBI vide circular dated May 22, 2008 has clarified that Cash transaction reporting by branches to their controlling offices should be submitted on monthly basis and not on fortnightly basis.



While the circular provides both manual as well as electronic formats for submission of CTR, banks have been advised to initiate urgent steps to ensure electronic filing of CTR.

In case of Banks who have implemented software solutions for AML, CTR generation module forms part of the standard suite of the software.

Some Banks who have not availed of AML software may require their technology departments to institute suitable procedures for extraction of data and arranging the same in form of text files in specified format every month.

The FIU-IND has provided an excel based utility at its website www.fiuindia.gov.in for generation of CTR in electronic form. This could be used by banks who do not have a core banking system. After following steps instructed by FIU-IND therein, the said utility automatically generates a set of 6 files for onward reporting to FIU-IND.

Banks on CBS find it relatively easier to report the CTR. However other banks would have to ensure that the generation of CTR is a centralised activity and therefore their processes have to facilitate timely collation of data across all branches at one location so that reporting can be done.

Banks are required to incorporate the BSR code in the Branch file of the CTR and this is also necessary as part of the format to be incorporated in the CBAACC, CBAINP and CBALPE for cross-referencing. In case BSR is not available in case of new branches, banks may use a unique code other than BSR for the branch so that it is possible to identify records across the CTR files.

5.3 Counterfeit Currency Reporting (CCR)

The PMLA Rule 3(1)(C) read with rule 8 requires the reporting of all cash transactions where forged or counterfeit Indian currency notes have been used as genuine. The RBI vide circular dated May 22, 2008 provided the format in which the CCR needs to be reported to the FIU-IND. The said report is required to be filed not later than seven working days from the date of occurrence of such transactions.

Banks may enter data centrally on counterfeit currency into a separate



utility provided by FIU-IND for same. This utility is available on FIU-IND website. After following steps instructed by FIU-IND therein, this utility automatically generates a set of 3 files for onward reporting to FIU-IND.

For enabling CCR reporting banks would need to put in place a mechanism such that information on counterfeit currency flows to a central location for onward submission to FIU-IND through the principal officer.

It is necessary that each entry in the counterfeit currency report carries the details of the account in which such currency is deposited.

RBI vide circular dated May 22, 2008 provides that these cash transactions should also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

5.4 Suspicious Transaction Report (STR)

The PMLA Rule 3(1)(D) read with rule 8 requires the reporting of all suspicious transactions whether or not made in cash.

It may be noted that the process for arriving at suspicious transaction is covered separately in the chapter on transaction monitoring. In this section we have only dealt with the modalities of reporting an STR.

RBI circular dated February 15, 2006 requires that the Suspicious Transaction Report (STR) should be furnished within 7 days of arriving at a conclusion that any transaction, is 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. The said circular also provides the format of the STR.

FIU-IND has provided a utility at its website for generation of STRs in electronic formats. On following steps instructed by FIU-IND therein, the said utility automatically generates a set of 6 files for onward reporting to FIU-IND.

While furnishing the STR care needs to be exercised on drafting of the grounds of suspicion (GOS) in part 8 of the STR format. This part of the



STR is the 'Soul' of the STR as it answers the essential question of why the STR is being filed. Therefore the GOS have to be accurate and complete. The grounds of suspicion should express fully 'why' the transaction or activity is unusual, unjustified, does not have economic rationale, or bonafide purpose keeping in mind the banking business and services offered by the Bank. The GOS could also explain the relationship between persons (natural & legal), accounts and transactions that are being reported as part of the STR. Correct reason for suspicion needs to be identified as it signifies the character of suspicious activity. GOS need to be in form of a detailed paragraph justifying why the transactions are considered to be suspicious. Specific reference requires to be drawn to the customers profile, apparent financial standing, past activity in account, rationale/purpose behind the transactions, business profile and general transaction pattern etc. These grounds are indicative in nature and may vary from case to case. Findings of any other due diligence may also be mentioned in the GOS.

Subsequent to furnishing an STR the FIU-IND/ other investigative agencies to whom the STR is forwarded by FIU-IND, may seek additional inputs in form of documents such as Account opening form and KYC documents. Pertaining to the customer from the bank. Banks may therefore arrange to keep these documents ready for submission (if required).



Chapter 6

TRANSACTION MONITORING

6.1 What is Transaction Monitoring?

As mentioned in Chapter on reporting requirements, banks are required to report suspicious transactions to the FIU-IND. This requires the Banks to put in place a formal process for identifying suspicious transactions and a procedure for reporting the same internally. This process is known as transaction monitoring.

Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps the banks to know their customers, assess risk and provides greater assurance that the Bank is not being used for the purposes of financial crime. Thus monitoring means analysis of a customer's transactions to detect whether the transactions appear to be suspicious from an AML or CFT perspective.

Suspicious transactions are reported to the Financial Intelligence Unit, India (FIU-IND).

6.2 Methods of Monitoring

Banks need to have suitable mechanisms to identify suspicious transactions. The methods for monitoring may be broadly classified as follows:

- i) **Observation:** The staff at the bank's branches may at the time of processing the transaction or otherwise come across certain transactions not in line with the profile of the customer. Certain behaviour displayed by the customer during their interactions with such customer may also lead to suspicion. Banks may advise their branch staff to report such instances to the principal officers/ his representatives so that additional due diligence may be done on same. A list of behavioural indicators that should trigger suspicion is enclosed as **Annexure C**.
- ii) **Analysis of Exception Reports:** Banks may have in place a system of generation of exception reports at branches or at the central office to examine accounts based on certain threshold limits. Suitable due diligence may be conducted for these accounts and accounts



concluded to be suspicious may be reported to the FIU-IND through the principal officer.

- iii) **AML Software:** Banks may have an AML software to generate alerts / exceptions and then channel these alerts for suitable due diligence and reporting. Alerts concluded to be suspicious might be reported to the FIU-IND through the principal officer. RBI vide its circular dated May 22, 2008, as a part of transaction monitoring mechanism, requires banks to put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers.

6.3 What is a suspicious transaction?

As per PMLA Rule 2 (g) suspicious transaction means a transaction whether or not made in cash which to a person acting in good faith-

- a. gives rise to 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
- d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism

In determining whether the transaction is suspicious or not, Banks needs to have regard to the indicators of suspicion. Indicative lists of such indicators are listed in **Annexure D**.

Complex transactions having no economic rationale or bonafide purpose, concluded to be suspicious, need to be reported to FIU-IND. Banks need to put in place suitable systems to identify and report such transactions through transaction monitoring.

What are the essentials of transaction monitoring process?

An effective transaction monitoring process should contain the following necessary elements:

Identification of Exceptional transactions: Recognition of suspicious



transaction requires the banks to know which transactions it should analyze from the huge number of transactions they process. Therefore, based on above indicators of suspicion, banks need to devise business rules based on value, number and frequency. In advanced stages of an AML program, Banks may use customer profiles and historical activity to alert them on suspicion. Banks may also use predictive modeling at mature stages of AML implementation. This involves analyzing the salient features of suspicious activity reported in STRs by the bank and devise scenarios involving such features.

Analysis of transactions / available customer information: This involves scrutiny of the transactions carried out by the customer over a longer period of time, the basic KYC information available in the bank's systems as also checking on any unusual patterns or complexity in the transaction.

Enhanced Due diligence: In case the bank requires additional information on the customer for concluding the suspicion or otherwise, it may conduct an enhanced due diligence through the Branch manager or any other bank official having knowledge of the customer. Based on such customer information, objective parameters, judgment of business group, and banker's prudence, Banks arrive at a conclusion whether the transaction is suspicious or not. Some of the objective parameters which can be used for enhanced due diligence could be:

- a. Customer location
- b. Financial status
- c. Nature of business
- d. Purpose of transaction

Confirmation of Suspicion: In case the above process leads the Bank to conclude that transaction is suspicious, then the same would be reported to the principal officer who on confirmation of the suspicion would file a report onward to the FIU-IND in an STR.

6.4 Who should perform transaction monitoring?

Depending on the structure of the Bank, transaction monitoring may be either be based at branches or at centralized location. Alerts/exceptions



generated may be filtered by a central unit and then forwarded to business units/ branches having knowledge about the customer. In case of Branches not on core banking these exception reports/ alerts may be generated at the branch and analysed by the branch manager or designated officer.

6.5 What types of rules should be used for generation of exception

Banks may as per their internal policy in this regard and based on their assessment of risk use following types of rules based on threshold limits or patterns for generation of exception reports/alerts :

1. Pure thresholds:

- Large Value Cash Transactions
- Large Value Non Cash Transactions
- Large Volume of Transactions
- Large Value transaction in dormant accounts
- Large number of remittances
- Large value of remittances

2. Pattern checks:

- Single remitter transmitting funds to multiple beneficiaries
- Multiple remitters transmitting funds to single beneficiary
- Multiple accounts of the same customer
- Any other pattern, which appears unusual, based on banks experience

Profile based alerts:

Significant deviation from known transaction profile of customer

Note: Above are purely indicative in nature. Fine-tuning of these may be done based on typologies observed during the course of time.

6.6 Challenges in Transaction monitoring:

What is white listing? How does a bank manage white listing?



With threshold-based alerts, there may be instances where the same customer accounts repeatedly hit the threshold limit to generate alerts. This results in a large number of repeated alerts involving the same accounts. To deal with such situations the AML softwares provide a false positive manager which allows accounts to be white listed for a specified period of time if they are found to be non suspicious after due diligence.

6.7 Do banks need to Report attempted ML transactions

RBI circular No DBOD.AML.BC. No. 85/14.01.001/2007-08 dated May 22, 2008 has advised banks that in case a transaction is abandoned/ aborted by customers on being asked to give some details or provide documents, it should report all attempted transactions in STRs even if not completed by customers irrespective of the amount of transaction. Thus banks may need to issue instructions to its branches to note above during course of customer interaction.

6.8 Do banks need to File repeat STR

In case one STR has already been filed for a particular account and fresh alerts pertaining to the same account are observed, the Bank needs to exercise judgment as to whether it requires to be reported considering following factors :

- Has any additional ground of suspicion which has not been reported earlier, been discovered.
- Is the Alert value/volume/frequency is substantially high as compared to the earlier STR

6.9 How should Banks deal with reported accounts?

Reported accounts are required to be put on enhanced monitoring. These accounts should be classified as high risk. In case significant activity is observed in such accounts, a repeat STR may be triggered.

In case the STR is repeatedly reported, banks may consider closing the account. However customer should not be tipped off.

6.10 What is the key to an effective transaction monitoring process?

The following are key requirements of any transaction monitoring system:



1. Performing sufficient due diligence on the customer.
2. Documenting reasons for arriving at conclusion of alert/ exception as suspicious/ non suspicious.

6.11 Is it necessary to have software for AML transaction monitoring?

The RBI circular dated May 22, 2008 requires banks to have suitable software to throw alerts for transaction monitoring. Thus it is an important requirement for robust transaction monitoring system, especially in view of the high number of transactions that the banks handle everyday, which is making it increasingly difficult to monitor these through manual methods.

6.12 How does AML software operate?

An AML software solution provides the interface wherein data from Core banking system is uploaded into it on a periodical basis. Based on this information the software generates alerts, which need to be investigated by the Bank.

6.13 What are the features that should be available while selecting AML software?

Following are the minimum features which should be available as part of any AML software:

1. **Cash Transaction Report:** The system should be capable of generating automated Cash Transaction Reports to the Financial Intelligence Unit. It should also be up gradable to carry out online reporting as and when required by FIU-IND.
2. **Customer Risk Categorization:** The system should have a feature for automated customer risk categorization based on available parameters of customer information.
3. **Alerts Generation / Rule Engine:** The system should be capable of generating alerts based on rules specified therein. The alerts should be capable of being configured based on varied criteria such as customer segment, product type, and customer risk.
4. **Case Management:** The system should be flexible enough to be customized to suit the bank's requirement. The case management consists of features such as assignment/reassignment, attachment



facility, making comments and flexible templates for recording due diligence.

5. **Investigation Tools:** AML systems also have features for user to carry out multi dimensional analysis of data, viewing customer information, linked accounts, details of transactions.
6. **Suspicious Transaction Report:** The software should be capable of generating auto populated suspicious transaction reports for reporting of suspicious transactions to the Financial Intelligence Unit.
7. **Reports:** The software should be able to generate various transaction reports as also management information reports.

Besides above any software should be compatible with the core banking system and scalable and up gradable to meet the changing face of banking.

6.14 How can Banks institutions effectively implement AML monitoring software?

Immediate fallout of AML software implementation could be a very large number of alerts. Banks would need to fine-tune the systems and processes during the initial implementation phase. The AML and technology departments would need to work together to ensure stabilization of the system in the initial phases.

6.15 How can bank carry out due diligence without tipping off the customer?

As a general practice Banks are advised by RBI not to put any restrictions on operations in the accounts where an STR has been made. However, in case any restrictions are placed it should be ensured that there is no tipping off to the customer at any level.

Although the definition of tipping off has not been specified, tipping off would mean informing/communicating to the customer that his account has been or would be reported for suspicious activity to the regulators/ FIU-IND.

Merely seeking information about a particular transaction, as part of the due diligence should not tantamount to tipping off. This is so because



most customers are well aware of the statute on money laundering and legal provisions involving obligations of banks thereon.

Some of the suggestions to avoid tipping off are :

1. Due diligence should be preferably by way of pretext sales calls.
2. No statement should be made, which cautions or warns the customer.
3. AML triggers / rules / reporting thresholds and internal monitoring processes should not be discussed with the customers.
4. The conclusion that has been arrived at after making the necessary enquiries should not be revealed to the customer.
5. No disclosure should be made to the customers that his/her accounts are under monitoring for suspicious activities or that STR has been filed/is being filed against him.



Chapter 7

NAME SCREENING PROCESS

7.1 Defining Name Screening

Name screening refers to the process of determining whether any of the bank's existing or potential customers are part of any blacklists or regulatory lists.

Under the risk based approach, banks should also put in place procedures for conducting enhanced due diligence in dealings with customers under certain categories, who may be perceived to pose higher risk from Money Laundering and Reputation Risk Perspective (e.g. Politically Exposed Persons (PEPs), persons entities, located in high risk locations, etc.). Name screening is used to identify such individuals also.

7.2 Purpose of Name Screening

RBI Master Circular on Know Your Customer (KYC) Norms/Anti Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/Obligations of Banks under PML Act 2002 dated July 1, 2009 as part of the Customer Acceptance Policy makes it mandatory for banks to conduct 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 terrorist individuals or terrorist organizations.

Further, RBI circular notifying the rules under the Prevention of Money Laundering Act, 2002, dated February 15, 2006 indicated that the banks need to monitor transactions of the customers for the purpose of reporting suspicious transactions to the FIU-IND in the specified format named as 'Suspicious Transaction Report (STR)'. STR specifies one of the categories of suspicious transactions as "Background of the client", which means clients with suspicious background or links with known criminals.

RBI Master Circular also advises Banks that before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the consolidated list of terrorist individuals and entities circulated by RBI. Further Banks should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list.



In order to meet these regulatory objectives, name-screening process is required to be embedded as an essential element of the effective customer due diligence program. Additionally, name screening is also required to be performed at the transaction monitoring or customer review mechanism.

Apart from the regulatory requirements, name screening processes is also a safety mechanism used to guard against reputation, operational or legal risks and to prevent themselves being used as a channel for money laundering or terrorist financing purposes.

7.3 Scope of Screening

Name screening process should be performed for the following types of transactions:

- i. New customers should be screened at the time of opening of accounts.
- ii. Screening of legacy customers, i.e. screening of the bank's existing customers at regular intervals.
- iii. Employees are required to be screened as a part of their pre-recruitment process, besides screening the existing employees at regular intervals. Vendors and contractual staff may also be included as a part of the screening.
- iv. Counter parties to the cross border transactions (i.e. remitters, beneficiaries, intermediary banks, other intermediaries, etc.) in remittance or trade transactions need to be screened.
- v. It also needs to be a part of the enhanced due diligence for high-risk customers or suspicious transactions review.

7.4 Negative lists to use for name screening

As per extant RBI guidelines, banks are required to ensure that before opening any new accounts, proposed customers do not appear in the United Nations' List under Security Council Resolutions (mainly 1267 and such others as may be specified by RBI from time to time) and the terrorist lists circulated by RBI. All the UN resolutions published by RBI should be made available at the branches or the relevant processing centres where the account opening takes place.

Other lists issued by enforcement agencies may also be included in the negative lists suite, such as: Interpol Most Wanted, Central Bureau of Investigation, Lists issued under other Resolutions by United Nations, etc.



Banks may also follow a risk-based approach and depending upon jurisdictions they operate, they may include foreign regulators'/enforcement agencies negative lists for name screening purposes.

7.5 Need for software

In order to perform the name screening function in a timely manner and reduce dependency on manual processes, it is desirable that the name screening function be performed in an automated manner. Extent of automation would depend upon the following factors:

- a. risk policy of the institution
- b. volume of transactions
- c. turn around time available for processing of transactions
- d. availability of resources (capital, manpower, etc.)

Before establishing the name screening systems, following preparatory steps are required to be in place:

- Determine the category of lists to be included in screening universe.
- Decide about the timing of screening of transactions.
- Establish due diligence procedures and the process of conducting due diligence on the probable matches.
- Establish reporting procedures for confirmed matches.
- Estimate the number of matches at each stage and capacities concerned departments appropriately.

Selection of software and database vendors may involve following steps:

- Due diligence on the service provider
- Evaluation of logic used in name matching
- Check for suitability of workflow and modes of name screening (on-line, batch upload, etc.)
- Compatibility of database formats with the software



- Lists and category of names covered by the vendor
- Check for the frequency of updates being provided by the vendor and integration of the software to apply updates.
- Request a demonstration for usability, presentation and compatibility on formats provided by the Bank.
- Conduct pre-selection user level tests against simulated data to understand the functionality in full and likely impact on the systems.

7.6 Components of a name screening system & process

A typical name screening system will comprise of the following elements:

- Database:** The name screening software will scan the names against a database of derogatory lists, which the Bank will decide to use for scrubbing its customers or transactions. The lists may contain the following categories:
 - Regulatory lists
 - Politically Exposed Persons (PEPs) list
 - Other high risk categories' list

The Bank may decide to prepare and maintain its own list or subscribe to the lists provided by external vendors

- Application:** It refers to the software application which will consist of following components:
 - Name matching engine
 - Work flow tools
 - report generation utility for control and audit purposes
 - Front end interface for users and administrator
 - Interface with payment gateway or core banking system, etc.

7.7 Logic used for name screening

Name screening software's use different logic for searching a match against the negative list. Commonly used logic is fuzzy logic algorithms like Levenshettin or phonetic algorithms like Soundex.

Based upon the degree of closeness to the source name against a probable negative listed person, system allocates a score to the match. Based on



the nearness of the match, the algorithm would arrive at the score of the match. Minimum value of the match score is 1 and 100 is the maximum score. A match score of 100 indicates an exact match.

System can be configured to ignore matches below a certain threshold.

Loose or tight matching logic can also be applied to arrive at the right balance of false positives as per Bank's own judgment. The process of fixing the threshold or matching logic should be done after detailed tests and should be controlled at the Principal Officer level.

7.8 Dealing with name matches

The name screening application provides a list of the probable matches; which contain the source data against the probable names matching in the negative lists with their details (such as name, age/date of birth, address, nationality, offence, listing authority, etc.). A confirmed name match is termed as a 'true positive match' whereas others are termed as 'true negative match'.

A 'false positive match' is the matching of two individuals having different identities. Conversely, 'false negative match' indicates matching of the same individual but adjudged as a false match. 'False positive' requires additional research but the 'false negative' might trigger an investigation, penalties, legal fees, reputation damage, etc.

Due to the negative correlation and probable risks, systems and processes should be designed to eliminate 'false positives' but not at the cost of 'false negatives'.

The following grid can be used to determine a 'true' or 'false' match:

Details	Criteria
Date of Birth	Any two details to match with name (listed name or alias)
Place of Birth	
City	
Nationality	
Passport No; SSN; Driving License; etc.	Single match

False positives can be reduced by deploying white-listing functionality. It refers to the process of adding a customer to the accept list against the given negative listed persons. If the same customer is scanned subsequently, the system will not show a match against the previously white-listed profiles against that customer. Any changes in the white-listed customer record or entity listing should trigger the screening process afresh.

7.9 Reporting confirmed matches on Regulatory Lists

Once it is concluded that the match found is 'true', following actionable are suggested. However, these are indicative steps only and may vary depending upon the Bank's policy in this regard:

Match against	Suggested action
Individuals or Entities	<ul style="list-style-type: none"> • Stop the transaction or account opening activity. (If account is already opened, close the account.) • Report
Banks/Country	<ul style="list-style-type: none"> • As per the Bank's risk based policy, respective sanction program being adhered to by the Bank and applicable regulations.

In addition to the details of the matched entity, the account opening and customer identification documents also need to be forwarded to the Principal Officer.

7.10 Roles and responsibility of the Principal Officer

The Principal Officer of the bank is the single point contact for reporting of suspicious transactions to FIU-IND and/or RBI. Thus, all internal cases should culminate at Principal Officer's office for onward reporting by the Bank.

Based on the review of the relevant documents, the Principal Officer shall decide whether the transaction or account or applicant needs to be reported to the appropriate authorities. The reports shall be in the format prescribed by the FIU-IND.

Once the Principal Officer concludes a transaction/customer to be suspicious, he is responsible to report the case in Suspicious Transaction Report (STR) format within 7 working days (after confirmation of suspicion) to the Director, FIU-IND in the STR format.



7.11 Guidelines to avoid Tipping Off

PMLA mandates that the STR related information should not be revealed to the customers to avoid prejudicing or affecting an investigation, which may be initiated by the law enforcement agencies.

Thus, it is essential that all of the aforesaid activities of reporting of the confirmed matches are kept strictly confidential.

Records of all such reports and investigations should be kept securely and separately so as not to mix with general transactional data. Custody of such records may be entrusted with staff of sufficient seniority or responsibility.

Customers should not be informed of any such reports in any circumstances to avoid 'TIPPING OFF' offence.

7.12 Due Diligence Procedures for High Risk Category Matches

While the process stated in point no. 1 to 10 is followed for screening against regulatory lists. The same process can be observed for identification of High Risk Customers (like Politically Exposed Persons (PEPs) matches, Fraudsters, etc.).

As per extant guidelines, PEPs are defined as the individuals who are or have been entrusted 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. PEPs' definition includes the family members or close relatives of the individuals identified as above.

The regulatory guidelines mandate that the Banks should classify such customers in higher risk category. Higher level of scrutiny or enhanced due diligence (EDD) should be conducted while enrolling such customers and accounts should be monitored closely for transaction monitoring purposes and review of KYC at regular intervals. The decision to open PEPs' or any other high-risk account should be taken at a senior level, preferably in concurrence with Principal Officer.

Suggested EDD measures for PEP customers include the following:

- checking for any adverse information on such individuals or entities available in public domain,

- checking for sources of funds proposed to be routed/invested through the bank,
- tighter threshold for monitoring of transactions through these accounts,

frequent review of relationships and accounts for keeping KYC information up-to-date.



Chapter 8

WIRE TRANSFERS - FATF SR VII COMPLIANCE

- 8.1** Banks use wire transfers as an expeditious method for transferring funds between bank accounts. The wire transfer could be domestic or cross border. The beneficiary and originator could also be the same person.
- 8.2** **Domestic wire transfer** means any wire transfer where the originator and beneficiary are located within the same country. A transaction involving a chain of wire transfers that take place within the borders of a single country is domestic wire transfer even though the system used for effecting the transaction is located outside the country.
- 8.3** **Cross-border transfer** means any wire transfer where the originator and the beneficiary bank or financial institution are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.
- 8.4** Wire transfers, because of its capability of transferring funds instantaneously between geographies, have become the preferred mode of transfer of funds across the globe. In addition, because of the lesser human intervention in the transfer and hence lesser scrutiny, it also becomes a preferred route for criminals and terrorists to transfer their funds. To address this, FATF in its Special Recommendations to combat terrorist financing made recommendations of some minimum requirements for the wire transfers. RBI vide its circular dated 13 April 2007 implemented the recommendations in the banks in India.
- 8.5** **Requirements for Domestic Transactions:**
- (a) Information accompanying all domestic wire transfers of Rs.50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.
 - (b) If a bank has reason to believe that a customer is intentionally structuring wire transfer to below Rs.50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the bank must insist on complete customer identification before effecting



the transfer. In case of no cooperation from the customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be made to FIU-IND.

- (c) When a credit or debit card is used to effect money transfer, necessary information as (a) above should be included in the message.

8.6 Requirements for Cross-border Transactions:

- (a) All cross-border wire transfers must be accompanied by accurate and meaningful originator information.
- (b) Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included.
- (c) Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (b) above.

8.7 Inter-bank transfers and settlements where both the originator and beneficiary are banks or financial institutions are exempted from the above requirements.

8.8 Role of Ordering, Intermediary and Beneficiary Banks

(i) Ordering Bank

An ordering bank is the one that originates a wire transfer as per the order placed by its customer. The ordering bank must ensure that qualifying wire transfers contain complete originator information. The bank must also verify and preserve the information at least for a period of ten years.

(ii) Intermediary Bank

For both cross-border and domestic wire transfers, a bank processing an intermediary element of a chain of wire transfers must ensure that all originator information accompanying a wire transfer is retained



with the transfer. Where technical limitations prevent full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record must be kept at least for ten years (as required under Prevention of Money Laundering Act, 2002) by the receiving intermediary bank of all the information received from the ordering bank.

(iii) Beneficiary Bank

A beneficiary bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they should be reported to the Financial Intelligence Unit-India. The beneficiary bank should also take up the matter with the ordering bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information on the remitter, the beneficiary bank should consider restricting or even terminating its business relationship with the ordering bank.

- 8.9** While the information as required above will enable banks to furnish the details to authorities in an expeditious manner for investigation or prosecution of money laundering or terrorist financing cases, the beneficiary banks also should analyse the data to find out any unusual/ suspicious activities which they may consider reporting to the FIU-IND India.



Chapter 9

STAFF AND CUSTOMER AWARENESS

9.1 Why is it important to create staff awareness

One of the most important controls over the prevention and detection of money laundering is to have staff members who are alert to the risks of money laundering/terrorist financing and well trained in the identification of unusual activities or transactions, which may prove to be suspicious. The effective application of even the best-designed control systems can be quickly compromised if the staff members applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of the bank's AML/CFT strategy.

9.2 How should the staff awareness be created

Responsibilities of the senior management

The senior management of the Bank should provide appropriate training to the staff members, specifically to those working in high-risk areas, e.g. branches, remittances etc on how to recognize and deal with transactions which may be related to money laundering or terrorist financing.

Responsibilities and obligations of staff

Please refer to Section 2.2 of this document.

Training methods and assessment

Induction training in money laundering prevention, recognition and reporting of suspicions and the KYC requirement should be given to relevant staff at the start of their employment in that role. Relevant staff members are those who handle or are managerially responsible for handling transactions, which may involve money laundering. On-going training / information must then be given to relevant staff at appropriate intervals to keep them abreast with developments in the area of AML.

Banks need to take appropriate measures so that relevant employees are aware of-

- a. Policies and procedures put in place to prevent money laundering.



- b. The legal requirements contained in the PMLA and the rules and regulations framed there under.
- c. KYC/AML guidelines issued by the RBI from time to time.

Banks are required to take reasonable steps to ensure that staffs who handle or are responsible for the handling of transactions which may involve money laundering, are aware of:

- a. their responsibilities under the Bank's arrangements for money laundering prevention including those for obtaining sufficient evidence of identity, recognising and reporting knowledge or suspicion of money laundering activity.
- b. findings on countries with a poor record in their anti money laundering legislations/regulations and their implementation (e.g. FATF notified list of NCCT).
- c. the identity and responsibilities of the PO.
- d. the potential effect on the bank, on its employees and its customers, of any breach of law.

All relevant staff should be made aware of the importance of the KYC requirements for money laundering prevention purposes. The creation of awareness and training of staff in this respect should cover:

- a. the need to know the true identity of the customer.
- b. where a business relationship is being established, the need to know enough about the nature of business activities expected in relation to that customer.
- c. at the outset to know what might constitute suspicious activity at a future date and the circumstances that would give rise to reasonable grounds for suspicion.

Records of training

It is the responsibility of senior management to ensure that their staff members have taken appropriate training and records are properly maintained. To this effect, any system report or manual (attendance) records can be maintained, which should be available for review by the RBI or other regulatory bodies.



It is important that training for relevant staff is made mandatory and that, in addition to the records of staff training, the Bank is required to maintain record of the date and nature of the training received.

9.3 Why is it important to create customer awareness on AML

In order to have an adequate control over AML, it is critical that key AML controls, such as KYC checks, have the support of industry and customers. Customers should see the KYC checks process as a sensible contribution to the fight against crime and terrorism and not as a burdensome and deliberate barrier to the access to banking. To promote this understanding, KYC checks should be done in a customer-friendly way and Banks' procedures and staff training should be designed accordingly.

9.4 How to create customer awareness on AML

There needs to be an effective communication to the customers of the reasons for KYC checks and what it normally involves. This could be done by various mediums, e.g.

- incorporating the requirements in the account opening forms;
- provision of relevant training to staff members to address any customer queries;
- a ready reckoner on frequently asked questions related to KYC should be visibly displayed on the notice boards;
- publishing relevant information on the websites of the bank;
- advertising AML/KYC related information on posters of the bank, which should be prominently visible.
- Customer awareness articles in newspapers and other media.



Chapter 10

PRESERVATION OF RECORDS

Section 12 of the PMLA 2002 makes it mandatory for every bank to maintain a record of all transactions, the nature and value of which may be prescribed.

10.1 Why is it important to maintain records?

The keeping of proper records is essential to enable the Banks to demonstrate that they have operated in conformity with local laws and regulations. This will in turn enable the Banks and individual staff members to defend themselves against any allegations of knowingly assisting a money launderer. Banks must retain records concerning customer identification and transactions as evidence of the work they have undertaken in complying with their legal and regulatory obligations, as well as for use as evidence in any investigation conducted by law enforcement.

It is important for the bank at all stages in a transaction to be able to retrieve relevant information, to the extent it is available, without undue delay.

10.2 What is record keeping?

Record keeping is an essential component of the audit trail that the regulators seek to establish in order to assist in any investigation and to ensure that criminal funds are kept out of the banking system.

10.3 What records have to be kept ?

The investigating authorities need to ensure a satisfactory audit trail for suspected money laundering transactions and to be able to establish a financial profile of the suspect account. For example, to satisfy these requirements the following information may be sought by the investigating authorities:

- the beneficial owner of the account;
- the volume of funds flowing through the account;
- for selected transactions:



- a) the origin of the funds (if known)
- b) nature of the transactions;
- c) the amount of the transactions and the currency in which it was denominated.
- d) the date on which the transaction was conducted;
- e) the form in which the funds were offered or withdrawn i.e. cash, cheque etc;
- f) the identity of the person undertaking the transaction;
- g) the parties to the transaction;
- h) the destination of the funds; and
- i) the form of instruction and authority.

10.4 What are the timelines for retention of records?

As per the PMLA, the account opening records including identification documents should be kept for 10 years from the date of cessation of the transactions/relationship between the customer and the bank and transaction records including credit/debit slips, cheques and other forms of vouchers (for account holders and non-account holders) should be kept for 10 years from the cessation of the transaction. Records relating to investigations and transactions, which have been the subject of a disclosure, should be kept for 10 years from the time the STR is filed with FIU-IND. Such records and related documents should be made available to help auditors in their work relating to scrutiny of transactions and also to RBI/other relevant authorities.

The term 'cessation' would broadly mean the time of closure of account. However, there may be certain exceptions to this, for example:

- a. If the matter related to a suspicious transaction is pending in a court, the relevant records should be retained for 10 years from the date of final verdict of the court.
- b. In specific cases, where RBI/FIU-IND or any other regulatory body requests for the retention of records for a period more than 10 years, the banks should be guided by such specific requests.



Mobile No. _____ Email _____

Mailing Address: Residence : _____

Office : _____

- Education :** Under Graduate Graduate
 Post Graduate Professional
- Occupation :** Salaried* Business#
 Self Employed# Retired / Housewife Student

Other (Please specify) :

*Name of Employer / #Line of Business / Industry
 (Please provide details) :

- Income p.a. :** Rs. 60,000 Rs. 60,000 to Rs. 100,000
 Rs. 100,000 to Rs. 500,000
 Rs. 500,000 to Rs. 1,500,000 Rs. 1,500,000

- Source of Funds :** Salary Business Inheritance
 Investments Other (Please specify)

Existing Account Number 1.

Existing Card Number 2.

2nd Applicant / Guardian Details:

If the first applicant is a minor For Bank use only

Mr. / Ms. / Mrs. _____

Title Surname First Name Middle Name

Date of Birth : _____ Gender : Male Female

Nationality : _____

PAN / GIR Number _____ If you do not have a PAN / GIR
 Number please fill in the following:

Are you an Income Tax Assessee? Yes No

If yes 1. Details of the Ward / Circle Range where the last return of income



was filed

2. Reasons for Not having a PAN / GIR No. _____

Residential Address

(If different from 1st App.)

Landmark : _____

Landmark : _____

City : _____ Pincode : _____ State :

Office Address : _____

Landmark : _____

City : _____ Pincode : _____ State : _____

Res Tel No. _____ Office Tel No. _____ Extn. : _____

STD Code _____ STD Code _____

Mobile No. _____

Mobile No. _____ Email _____

Mailing Address: Residence : _____

Office : _____

Occupation : Salaried* Business# Self Employed#
 Retired / Housewife Student Other (Please specify):

*Name of Employer / #Line of Business / Industries (Please provide details)

Source of Funds : Salary Business Inheritance
 Investments Other (Please specify)

Existing Account Number 1.

Existing Card Number 2.

Rel. with the 1st Holder :

Parent / Parent in Law / Spouse / Child / Sibling / Other

3rd Applicant Name :



(If applicable)

4th Applicant Name :

(If applicable)

Mode of operation : Singly / Jointly / Either or Survivor

Customer Benefits :

1st Holder :

2nd Holder :

Debit / ATM Card:

Regular Name as it should appear on card

Photo Debit Card - Please fill a separate form

Please leave a space between two words

Cheque Book : Local or Multicity

Internet banking

1st Applicant Yes No

2nd Applicant Yes No

If yes, email address must be provided on page 1

E-statements: Yes No

If yes, email address must be provided on page 1

Nomination :

Form DA1 Nomination under Section 45ZA of the Banking Regulation Act 1949 and Rule 2(1) of the Banking Companies (Nomination) Rule 1985 in respect of Bank deposits.

I/We nominate the following person to whom in the event of my/our/ minor's death, the amount of the deposit in the account, particulars, whereof are given below, may be returned by _____

Bank _____ Branch _____ Deposit/Account: _____

Nature of Deposit _____



Distinguishing No. _____

Additional Details if any _____

Full Name of the Nominee : _____

Date of Birth : _____ Relationship with the depositor _____

Address of the Nominee _____

(If different from First App.)

**As the nominee is a minor on this date I/We appoint

Guardian's Address : _____

to receive the amount of the deposit on behalf of the nominee in the event of my/our minor's* death during the minority of the nominee.

*Signature of the
First Applicant

*Signature of the
Second Applicant

If the account is in more than 2 names, do not complete this nomination form but complete the nomination form in the supplementary account opening form.

Witness Name

Witness Name

Signature***

Signature***

Address

Address

Date

Date

* where the deposit is made in the name of a minor the nomination must be



signed by a person lawfully entitled to act on behalf of the minor. **Strike out if not a minor *** Thumb impressions must be attested by two witnesses.

Customer Instructions

Initial Deposit Details : Rs. _____ (amount in words) _____

Cash/Cheque No. _____ Dated _____

Drawn on (Bank Name) _____

Debit to Account No _____

Please note all Cheques should be CROSSED and in favour of _____

_____ A/C (Your Name)

Term Deposit Tenure _____ Days _____

Months _____ Years _____

Maturity Instructions _____ Auto Renewal _____

Credit A/C No. _____

Issue a P/O favg. _____ (One of the account holders) _____

Interest Payment _____ Renew with Principal _____ Credit A/C No. _____

Issue a P/O favg. _____ (One of the account holders) _____

Signature

Signature

Name _____ Name _____

If the signature above does not tally with that on the ID Document please confirm that you want the signature to be recorded as per above by signing as per the identity document.

Date

Please submit a passport size photo for all holders signed on the face/reverse with the documents.

For Bank use only.



Annexure B

Non-Resident Individual Account Opening Form

Please open the following account(s) for me / us at (Branch)

Please fill the form in CAPITAL LETTERS. Please additionally complete the supplementary form in case of more than 2 applicants. Please do not staple this form.

Product Choice

- Savings Account NRO Savings NRE Savings NRE Super Value
- Term Deposit NRO (FD) NRE (FD) NRO Re-
Investment Deposit
- NRE Re-Investment Deposit FCNR Deposit Others

Customer Details - 1st Applicant

Mr. / Ms. / Mrs. _____

Title Surname First Name Middle Name

Date of Birth : _____ Gender : Male Female

Nationality : _____

Overseas Residential Address _____

(If P.O. Box address, Landmark is compulsory)	Landmark Pincode	City State	Country
--------------------------------------------------	---------------------	---------------	---------

Overseas Office Address _____

(If P.O. Box address, Landmark is compulsory)	Landmark Pincode	City State	Country
--------------------------------------------------	---------------------	---------------	---------

Mailing Address _____

(If different from any of	Landmark	City
---------------------------	----------	------



the addresses above) Pincode State Country

Res Tel No. Office Tel No. Extn
 STD Code STD Code
 Mobile No. Email

Mailing Address
 Residence Office Mailing

Education : Under Graduate Graduate
 Post Graduate Professional

Occupation : Salaried* Business#
 Self Employed# Retired / Housewife Student

Other (Please specify) :

*Name of Employer / #Line of Business / Industry

(Please provide details) :

Income p.a. : Rs. 60,000 Rs. 60,000 to Rs. 100,000
 Rs. 100,000 to Rs. 500,000
 Rs. 500,000 to Rs. 1,500,000 Rs. 1,500,000

Source of Funds : Salary Business Inheritance
 Investments Other (Please specify)

Existing Account Number 1.
 Existing Card Number 2.

2nd Applicant / Guardian Details:

If the first applicant is a minor For Bank use only

Mr. / Ms. / Mrs. _____

Title Surname First Name Middle Name

Date of Birth : _____ Gender : Male Female

Overseas Residential Address
 (If different from 1st App.)

Landmark : City :
 Pincode : State : Country



Overseas Mailing Address _____
(If different from 1st App.)

Landmark : City :
Pincode : State : Country
Res Tel No. Office Tel No. Extn. :
STD Code STD Code
Mobile No. Email

Mailing Address

Residence

Occupation : Salaried* Business# Self Employed#
 Retired / Housewife Student Other (Please specify):

*Name of Employer / #Line of Business / Industry (Please provide details)

Source of Funds : Salary Business Inheritance
 Investments Other (Please specify)

Existing Account Number 1.

Existing Card Number 2.

Rel. with the 1st Holder :
Parent / Parent in Law / Spouse / Child / Sibling / Other

3rd Applicant Name :

(If applicable)

4th Applicant Name :

(If applicable)

Mode of operation : Singly / Jointly / Either or Survivor

Customer Benefits :

1st Holder :

2nd Holder :

Debit / ATM Card :



Regular Smart Fill ATM Regular Smart Fill ATM

Name as it should appear on card

Photo Debit Card - Please fill a separate form

Please leave a space between two words

*Issued only on NRE transaction account; conditions apply

Customer Benefits

Cheque Book	Re-Order Automatic	Yes/No
Internet banking	1st Applicant	Yes/No
	2nd Applicant	Yes/No

(Only available if you have

If yes, email address must be provided on page 1

Current/Savings A/C with us)

E-statements Yes/No

If yes, email address must be provided on page 1

Nomination Form DA1 Nomination under Section 45ZA of the Banking Regulation Act 1949 and Rule 2(1) of the Banking Companies (Nomination) Rule 1985 in respect of Bank deposits.

I/We nominate the following person to whom in the event of my/our/ minor's death, the amount of the deposit in the account, particulars, where of are given below, may be returned by

Bank _____ Branch _____

Deposit/Account: Nature of Deposit

Distinguishing No. Additional Details if any

Full Name of the Nominee _____

Date of Birth _____ Relationship with the depositor _____

Address of the Nominee _____

(If different from First App.)

**As the nominee is a minor on this date I/We appoint



Guardian's Address _____

to receive the amount of the deposit on behalf of the nominee in the event of my/our minor's* death during the minority of the nominee.

*Signature of the First Applicant *Signature of the Second Applicant

If the account is in more than 2 names, do not complete this nomination form but complete the nomination form in the supplementary account opening form.

Witness Name

Witness Name

Signature***

Signature***

Address

Address

Date

Date

* where the deposit is made in the name of a minor the nomination must be signed by a person lawfully entitled to act on behalf of the minor. **Strike out if not a minor *** Thumb impressions must be attested by two witnesses.

Customer Instructions

Initial Deposit Details : Rs./USD/GBP/EUR

(amount in words)

Cash (Cash option not available for Indian Rupees)

Cheque No. Dated

Drawn on (Bank Name) Debit to Account No

Please note all Cheques should be Crossed and in favour of A/C (Your Name)

Term Deposit Tenure Days _____ Months _____ Years

Maturity Instructions Auto Renewal Credit A/C No. _____

Issue a P/O favg. _____ (One of the account holders)



Interest Payment Renew with Principal Credit A/C No. _____

Issue a P/O favg. _____ (One of the account holders)

It is my/our responsibility to obtain the terms and conditions from your bank and read the same. I/We confirm that all information given in this application form is true, correct, complete and upto date in all respects and I/We have not withheld any information. I/We shall be held responsible for the same at all times if it is incorrect. I/We confirm having read and understood the Rules and Regulations of the Bank including Bank's tariff regarding the conduct of the account/deposits and pertaining to Phone Banking, ATM, Debit Card, Internet Banking and Electronic Banking facilities (collectively called "the said banking facilities") and agree to be bound and abide by them/any other rules that may be in force from time to time. I/We confirm being persons of Indian origin not residing in India. I/We understand that the above account/deposit will be opened on the basis of statements made by me/ us. I/we also confirm that my/ our residential status as per Indian Income Tax Act 1962, in Non Resident Indian and I/ we agree and undertake to inform the Bank in writing of any change in residential status. I/We undertake to strictly operate and use the account/deposit and the said banking facilities in accordance with the Exchange Control Regulations as laid down by RBI from time to time.

Declaration under Section 10 (5) of FEMA 1999: I/We hereby declare that all foreign exchange transactions as may be entrusted by us to the Bank from time to time do not involve and are not designed for the purpose of any contravention or evasion of the provisions of the aforesaid Act or of any rule, regulation, notification, direction or order made thereunder. I/We also hereby agree undertake to give such information/documents as will reasonably satisfy you about the transaction in terms of the above declaration. I/We also understand that if I/We refuse to comply with any such requirement or make only unsatisfactory compliant therewith the Bank shall refuse in writing to undertake the transaction and shall if it has reason to believe that any contravention/evasion is contemplated by me/us report the matter to RBI.

Signature
Name

Signature
Name



If the signature above does not tally with that on the ID Document please confirm that you want the signature to be recorded as per above by signing as per the identity document.

#

#

Date

Please submit a passport size photo for all holders signed on the face/reverse with the documents.

For Bank use only

**Annexure C****Customer Behaviour Indicators**

- Customers who are reluctant in providing normal information while opening an account, providing minimal or fictitious information or when applying to open an account, providing information that is difficult or expensive for the institution to verify.
- Customer expressing unusual curiosity about a secrecy of information involved in the transaction.
- Customers who decline to provide information that in normal circumstances would make the customer eligible for banking services.
- Customer giving confusing details about a transaction.
- Customer reluctant or refuses to state a purpose of a particular large / complex transaction/ source of funds involved or provides a questionable purpose and / or source.
- Customers who use separate tellers to conduct cash transaction or foreign exchange transactions.
- Customers who deposit cash / withdrawals by means of numerous deposit slips / cheques leaves so that the total of each deposits is unremarkable, but the total of all credits / debits is significant.
- Customer's representatives avoiding contact with the branch.
- Customers who repay the problem loans unexpectedly.
- Customers who appear to have accounts with several institutions within the same locality without any apparent logical reason.
- Customers seeks to change or cancel a transaction after the customer is informed of currency transaction reporting / information verification or record keeping requirements relevant to the transaction.
- Customer regularly issues large value cheques without balance and then deposits cash.



Annexure D

An Indicative List of Suspicious Activities

Transactions Involving Large Amounts of Cash

- (i) Exchanging an unusually large amount of small denomination notes for those of higher denomination;
- (ii) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;
- (iii) Frequent withdrawal of large amounts by means of cheques, including traveller's cheques;
- (iv) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;
- (v) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;
- (vi) Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company, e.g. cheques, letters of credit, bills of exchange etc.;
- (vii) Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.

Transactions that do not make Economic Sense

- (i) A customer having a large number of accounts with the same bank, with frequent transfers between different accounts;
- (ii) Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.

Activities not consistent with the Customer's Business

- (i) Corporate accounts where deposits or withdrawals are primarily in cash



rather than cheques.

- (ii) Corporate accounts where deposits & withdrawals by cheque/telegraphic transfers/foreign inward remittances/any other means are received from/made to sources apparently unconnected with the corporate business activity/dealings.
- (iii) Unusual applications for DD/TT/PO against cash.
- (iv) Accounts with large volume of credits through DD/TT/PO whereas the nature of business does not justify such credits.
- (v) Retail deposit of many cheques but rare withdrawals for daily operations.

Attempts to avoid Reporting/Record-keeping Requirements

- (i) A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
- (ii) Any individual or group that coerces/induces or attempts to coerce/induce a bank employee not to file any reports or any other forms.
- (iii) An account where there are several cash deposits/withdrawals below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.

Unusual Activities

- (i) An account of a customer who does not reside/have office near the branch even though there are bank branches near his residence/office.
- (ii) A customer who often visits the safe deposit area immediately before making cash deposits, especially deposits just under the threshold level.
- (iii) Funds coming from the list of countries/centers, which are known for money laundering.

Customer who provides Insufficient or Suspicious Information

- (i) A customer/company who is reluctant to provide complete information



regarding the purpose of the business, prior banking relationships, officers or directors, or its locations.

- (ii) A customer/company who is reluctant to reveal details about its activities or to provide financial statements.
- (iii) A customer who has no record of past or present employment but makes frequent large transactions.

Certain Suspicious Funds Transfer Activities

- (i) Sending or receiving frequent or large volumes of remittances to/from countries outside India.
- (ii) Receiving large TT/DD remittances from various centers and remitting the consolidated amount to a different account/center on the same day leaving minimum balance in the account.
- (iii) Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire/funds transfer.

Certain Bank Employees arousing Suspicion

- (i) An employee whose lavish lifestyle cannot be supported by his or her salary.
- (ii) Negligence of employees/willful blindness is reported repeatedly.

Some examples of suspicious activities/transactions to be monitored by the operating staff-

- Large Cash Transactions
- Multiple accounts under the same name
- Frequently converting large amounts of currency from small to large denomination notes
- Placing funds in term Deposits and using them as security for more loans
- Large deposits immediately followed by wire transfers
- Sudden surge in activity level
- Same funds being moved repeatedly among several accounts



- Multiple deposits of money orders, Banker's cheques, drafts of third parties
- Multiple deposits of Banker's cheques, demand drafts, cross/ bearer cheques of third parties into the account followed by immediate cash withdrawals
- Transactions inconsistent with the purpose of the account
- Maintaining a low or overdrawn balance with high activity

Check list for preventing money-laundering activities:

- A customer maintains multiple accounts, transfer money among the accounts and uses one account as a master account from which wire/funds transfer originates or into which wire/funds transfer are received (a customer deposits funds in several accounts, usually in amounts below a specified threshold and the funds are then consolidated into one master account and wired outside the country).
- A customer regularly depositing or withdrawing large amounts by a wire transfer to, from, or through countries that are known sources of narcotics or where Bank secrecy laws facilitate laundering money.
- A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer's business or history.
- A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.
- A customer experiences increased wire activity when previously there has been no regular wire activity.
- Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.
- A business customer uses or evidences or sudden increase in wire transfer to send and receive large amounts of money, internationally and/or domestically and such transfers are not consistent with the customer's history.
- Deposits of currency or monetary instruments into the account of a domestic trade or business, which in turn are quickly wire transferred abroad or moved among other accounts for no particular business purpose.
- Sending or receiving frequent or large volumes of wire transfers to and



from offshore institutions.

- Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.
- Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency
- Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.
- Periodic wire transfers from a person's account/s to Bank haven countries.
- A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.
- A customer or a non-customer receives incoming or makes outgoing wire transfers involving currency amounts just below a specified threshold, or that involve numerous Bank or travelers cheques
- A customer or a non customer receives incoming wire transfers from the Bank to 'Pay upon proper identification' or to convert the funds to bankers' cheques and mail them to the customer or non-customer, when
 - The amount is very large (say over Rs.10 lakhs)
 - The amount is just under a specified threshold (to be decided by the Bank based on local regulations, if any)
 - The funds come from a foreign country or
 - Such transactions occur repeatedly.

A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Bankers' cheques (just under a specified threshold)

A Non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit.



Grounds of suspicion reported in STRs

(Extracted from the Annual Report of Financial Intelligence Unit -India (FIU-IND) for the year 2007-08)

Banking Companies

No.	Suspicion	Summary of detection and review
1	False Identity	Identification documents were found to be forged during customer verification process. The account holder was not traceable
2	Wrong Address	Welcome pack was received back as the person was not staying at the given address or address details given by the account holder were found to be false. The account holder was not traceable
3	Doubt over the real beneficiary of the account	The customer not aware of transactions in the account. Transactions were inconsistent with customer's profile.
4	Account of persons under investigation	The customer was reported in media for being under investigation.
5	Account of wanted criminal	Name of the account holder and additional criteria (Date of birth / Father's name / Nationality) were same as a person on the watch list of UN, Interpol etc.
6	Account used for cyber crime	Complaints of cyber crime were received against a customer. No valid explanation for the transactions by account holder.
7	Account used for lottery fraud	Complaints were received against a bank account used for receiving money from the victims. Deposits at multiple locations followed by immediate cash withdrawals using ATMs. No valid explanation provided by the account holder.
8	Doubtful activity	Cash deposited in a bank account at different



	of a customer from high risk country	cities on the same day. The account account holder a citizen of a high risk country with known cases of drug trafficking.
9	Doubtful investment in IPO	Large number of accounts involving common introducer or authorized signatory. A c c o u n t s used for multiple investments in IPOs of various companies.
10	Unexplained transfers between multiple accounts	Large number of related accounts with substantial inter-account transactions without any economic rationale.
11	Unexplained activity in dormant accounts	Sudden spurt in activity of dormant account. The customer could not provide satisfactory explanation for the transactions.
12	Unexplained activity in account inconsistent with the declared business	Transactions in account inconsistent with what would be expected from declared business. The customer could not provide satisfactory explanation.
13	Unexplained large value transactions inconsistent with client's apparent financial standing	Large value transactions in an account which usually has small value transactions. No valid explanation provided by the account holder.
14	Doubtful source of payment for credit card purchases	Credit card topped up by substantial cash first and then used for incurring expenses. Cumulative payment during the year was beyond known sources of income.
15	Suspicious use of ATM card	Frequent cash deposits in the account followed by ATM withdrawals at different locations. No valid explanation.
16	Doubtful use of safe deposit locker	Safe deposit locker operated frequently though the financial status of client



17	Doubtful source of cash deposited in bank account	Frequent cash transactions of value just under the reporting threshold. Cash transactions split across accounts to avoid reporting. No valid explanation provided.
18	Suspicious cash withdrawals from bank account	Large value cheques deposited followed by immediate cash withdrawals.
19	Doubtful source of foreign inward transfers in bank account	Deposit of series of demand drafts purchased from Exchange House abroad. Sudden deposits in dormant account immediately followed by withdrawals.
20	Doubtful remitter of foreign remittances	Name and other details of the remitter matches with a person on watch list.
21	Doubtful beneficiary of foreign remittances	Name and other details of the beneficiary matches with a person on watch list.
22	Doubtful utilizations of foreign remittances	Foreign remittance being withdrawn in cash immediately. No valid explanation.
23	Misappropriation of funds	Reports of misappropriation of funds. Substantial cash withdrawals in account of a charitable organizations.

Financial Institutions

24	Doubtful source of insurance	<ul style="list-style-type: none"> • Substantial premium paid by cash/demand draft in premium multiple insurance policies without valid explanation. • Substantial premium paid by multiple demand drafts of amounts below Rs.50,000. • Insurance premium much beyond declared sources of income.
25	Doubtful source of loan foreclosure	Substantial amount paid in cash / demand draft for foreclosure of loan account. No valid explanation provided.



26	Doubtful source of the inward foreign remittances	Inward foreign remittance received from a non relative. No valid explanation provided by the beneficiary.
27	Suspicious inward foreign remittances	Splitting of inward foreign remittances to collect funds in cash in an apparent attempt to avoid fund trail.
28	Doubtful beneficiary of foreign remittances	Doubtful credentials of the beneficiary. No valid explanation for the remittance provided.
29	Doubtful purchase of foreign exchange by a customer	Substantial foreign exchange purchased in cash or demand draft. No valid explanation provided.
30	Doubtful sale of foreign exchange	Substantial foreign exchange sold without any valid explanation.

Intermediaries

31	Doubtful source of investment in mutual funds	Substantial investment in multiple folios in short span. Form 60/61 provided for substantial investment. No valid explanation provided.
32	Doubtful ownership of investment in mutual funds	Large investment in mutual fund using third party cheques. No valid explanation provided.
33	Suspicious off market transactions in demat accounts	Off-market transfer of shares from multiple demat accounts to one demat account. No valid explanation provided. Suspected share price manipulation by bulk off-market transactions.

Annexure E

Anti-Money laundering - Case Studies of Suspicious Activities (Useful For Training Purposes)

Case Study 1

Mercury Leather Impex Pvt Ltd. deals in manufacture and export of rexin goods, as per the documents provided. Transactions in the account were normal with no inward or outward remittances. Customer receives an inward remittance of INR 5.5m and issues cheques for smaller amounts to various persons. Customer explains the transaction as proceeds of an export of wrist watches to Dubai. No proof shown regarding trading in wrist watches and no explanation given for the pay outs. Unusual transaction. Activity not in line with the known business/ source of funds - an apt case for raising a SAR.

Key Message

Continuously look out for transactions not in line with the customer's known business activity.

Case Study 2

ABC Tours & Travels is a customer. Manager of this company introduced a person for opening a current account. AR, the person introduced claims to have business in Canada and intending to start property business in the country. KS, the Asstt. Manager approves opening of the account on the basis of National Identity Card and Certificate of Registration of business issued by govt. Within a few days of opening of account, address changed. Initial address same as that of ABC Tours & Travels. Within a month of opening of account, 4 remittances from Canada totaling TBD 21M (USD 210K) received in the account. Followed by cash withdrawals. Most of the transactions were approved and/or were in the knowledge of the Asstt Branch Manager and the Branch Manager. Subsequent information revealed that the money was proceeds of a fraud perpetrated on the remitting bank. The owner of ABC Tours & Travels was arrested a few years back for suspected association with a terrorist group operating in the country. He was let off without framing any charges. This fact was known to the branch personnel. Inadequate KYC information about the new business. No enquiries/ verification regarding the claim of business in Canada. Large inward remittances in newly opened account followed by immediate withdrawals in cash - clear indicators to



raise suspicion. Change of address soon after opening account, another indicator for suspicion. Above indicators coupled with the information about the suspected involvement of the owner of ABC Travels & Tours Ltd. with a terrorist organisation should have raised suspicion at some stage.

Key Message

Do not let your judgment be influenced by extraneous matters like the introduction by a known person or tall claims of business activities else where. Always look for evidence to support the claims.

Case Study 3

RD Group, a well known group in city KK has non-borrowal relationship with the bank. Operated three main accounts, one a private limited co. and two partnership firms. Mr. RD is MD in the pvt. Ltd. co. and partner in others. Around 15 other accounts of the group where about 10 persons, believed to be employees of the group, operated the accounts as proprietors or partners in various combinations. Large cash deposits and very frequent inter-account transfers. I.T. made enquiries about operations in some of the accounts. During verification, it was found that addresses in some of the accounts were non-existent. Group explained that they sell goods to retailers and that generate cash and they are also in real estate business. Multiple accounts are maintained for efficient tax management. Since the transactions lacked transparency and verifications were negative, decided to exit relationship. Some of the existing accounts in the group were not KYC compliant. It was known to the staff in KK that all the 15 odd accounts were being operated as a group. They should have questioned the necessity of all these accounts and the transactions going through these accounts. SARs should have been raised, if proper explanation was not forthcoming on the transactions.

Key Message

Do not compromise compliance for revenue. Apply caution in case of regular inter group transfers with no apparent economic sense.

Case Study 4

Between May 2004 and October 2004 MA opens 12 accounts, seven individual accounts and 5 business accounts (MA as proprietor). Transactions large deposit of cash and withdrawals through ATMs or by cheque. Multiple accounts caused suspicion and SAR filed by one branch in November, 2004. On 2/12/04, BDD 2.8M



(USD 40K) deposited in to five of the accounts. The amount deposited came from cash withdrawal from another individual's account (SRC). The whole amount withdrawn in cash from all the accounts through various branches, the next day. Subsequently, it came to light that the amount was transferred to SRC account from a corporate account through fraudulent means. Lack of application of mind and caution while multiple accounts were opened. Nobody made enough enquiries to know the details of the business of the account holder or the necessity of his maintaining so many accounts. TR sourcing multiple accounts without really knowing the customers business and need for the accounts was not prudent. While allowing the cash withdrawal from the account of SRC and depositing this amount in the five accounts of MA, the concerned staff did not make enough enquiries regarding the purpose of the transactions but merely accepted some perfunctory explanations given. The officer allowing the above transaction should have gone through the transaction details in SRC account (a newly opened account) and probed the large credit in to this account

Key Message

Always look for the real purpose while opening multiple accounts and be careful about inter group transfers.

Case Study 5

GI was issued a credit card in January 2002 with credit limit INR 30,000. Some small transactions and payment through third party cheque drawn in favour of the card holder. Since April, 2004, payments through demand drafts issued in .Africa, etc. drawn in favour of various persons with endorsements authorising payment to GI's credit card account. Number of withdrawals in cash through ATMs and branches, high value purchases from jewelers, electronic shops, etc. Account continuously remained in credit. Fraud Control got alert due to high value transactions. Verified with customer who confirmed the transactions. Complaint from one of the beneficiaries of the draft led to the discovery that about 30 drafts for approx. INR 950,000 were fraudulently collected through the credit card account. Subsequent investigation revealed airline staff pilfered drafts from mail bags. The drafts should not have been credited in the account, as the endorsements were not valid. Authorisation while making the verification should have gone through the pattern of transactions in the account. There were indications such as large purchases from Jewelers, electronic goods shop and cash withdrawals that would have given suspicion about the transactions. The large credit balance and the odd figures of



deposit should also have given doubt about the transactions.

Key Message

While investigating an unusual or suspicious activity, go into all aspects and get satisfied before giving a go ahead. Do not simply rely on explanations / clarifications unless there are grounds to believe them.

Case Study 6

Money Transfers

The police arrested suspect A, the leader of an Iranian drug trafficking group, for possessing stimulants and other kinds of drugs. The subsequent investigation revealed that the suspect had remitted part of his illegal proceeds abroad. A total of US\$450,000 was remitted via three banks to an account on behalf of suspect as older brother B at the head office of an international bank in Dubai. Transfers were made on five occasions during a two-month period in amounts ranging from US\$50,000 to US\$150,000. Another individual, suspect C, actually remitted the funds and later returned to Iran. On each occasion C took the funds in cash to the bank, exchanged them for dollars, and then had the funds transferred. Each of the transactions took about one hour to conduct, and the stated purpose for the remittances was to cover "living expenses". Suspect A was initially charged with violating provisions of the anti-narcotics trafficking law. The money transfers revealed during the investigation led to additional charges under the anti-money laundering law.

Key Message

This case represents a classic example of a simple money laundering scheme and is also a good example of a case derived, not just from suspicious transaction reporting, but also as a follow-up to traditional investigative activity.

Case Study 7

Exchange transaction relates to laundered drug money and diamond smuggling.

A foreign exchange transaction of a European currency into US dollars for a value of almost US\$177,000 was reported to the FIU of an FATF member jurisdiction (Country A). At the time of the transaction, the individual, of Asian origin, gave the exchange office an address in another FATF country (Country B). This first



transaction was soon followed by four more similar transactions. After several weeks, the total had already attained US\$618,000. After a break of six months, the exchange transactions resumed. Over a four-month period, the intermediary appeared with large amounts in pesetas to be converted into dollars. The total amount of the transactions described in reports to the FIU amounted to more than US\$1.3mn.

The information obtained from law enforcement demonstrated that the individual had no criminal record in Country A. Given that the case involved large amounts for which there existed no apparently legitimate economic justification, the FIU pursued the investigation. Several foreign FIU were queried. One of them was able to provide useful information: the individual was known as a member of a group of drug traffickers who performed the same type of transactions in the country involved. Investigation of the members of this group was already in progress in this latter country. Secondly, it appeared that the address provided during the first contact with the financial institution was false. On the basis of these elements, the FIU decided to turn over the case file to the prosecutorial authority. The subsequent investigation showed that the individual had not been acting alone. For a number of years she had played a dominant role in money laundering transactions involving a total amount of around US\$11.5mn.

The individual was arrested in the company of one of her accomplices and in possession of a large sum in US dollars. She acknowledged the retail foreign exchange transactions, as well as the illicit origin of the funds. According to her account, they were derived from illegal diamond trafficking. She was sentenced to four years in prison (two of which were suspended) and a fine of nearly US\$1mn. The funds seized were confiscated, as well as the amounts exchanged; her accomplices were each sentenced to two years in prison (one of which was suspended).

Key Message

This example clearly illustrates the importance of international co-operation and the exchange of information between FIU and their foreign counterparts in the detection of money laundering transactions. It also demonstrates the necessity for financial institutions to continue sending suspicious transaction reports to the FIU, even when they do not at first seem to produce an immediate response from the authorities.



Case Study 8

Launderers recruit individuals for the use of their bank account.

An FIU received suspicious transaction reports from three financial institutions concerning international fund transfers. Through police investigation, it was discovered that several individuals were acting as money collectors for a cocaine trafficking organisation. The job of these individuals was to identify and "recruit" professionals already established in various trades and services who might be amenable to earning some extra money by allowing their bank accounts to be used in a laundering scheme. The professionals would place cash in their accounts and then transfer the sum to accounts indicated by the money collectors.

The professionals who became involved in this activity were active in several types of business, including travel agencies, and import/export in commodities and computers. In return for their services, they received a commission on the funds transferred through their accounts. The transfers out of the accounts were justified by fictitious invoicing that corresponded to their particular business.

This investigation uncovered an organisation that was laundering the proceeds of cocaine trafficking believed to be worth US\$ 30 million. Several members of the group were identified and tried in two countries.

Key Message

This scheme illustrates how criminals put additional measures into place further to distance the money from the narcotics trafficking operation. Cash is collected from the drug dealer; the collector passes the funds to the launderer; the launderer then passes them to the recruited business professional, who then transfers the funds abroad for further processing. The money continues to move, and the trail becomes more complex. The use of professionals can establish a 'break' in the trail, and so thwart financial investigators.

Case Study 9

Use of bank safety deposit boxes

A law enforcement investigation centred on the suspicious behaviour of a bank customer who appeared to be exchanging old, outdated banknotes for a new series of banknotes. The suspect appeared to be storing the old banknotes in one of the bank's safety deposit boxes.

The suspect received social security payments and had no other identifiable



legitimate income.

Further enquiries revealed that the suspect had an extensive criminal history and had recently purchased a motor vehicle with a large amount of cash and owned a number of high value real estate properties.

The investigation established that the suspect was involved in drug cultivation in the houses that he had purchased using the proceeds of his drug trafficking activities. The suspect was using the bank's safety deposit facilities to store cash obtained from the sale of the illegal drugs and also to store jewellery purchased with the same proceeds.

Key Message

This example illustrates that a complicated money laundering scheme is not always necessary to integrate illegal proceeds back into the circulation.

Case Study 10

Use of a bureau de change and bank accounts under false names

A drug trafficking investigation established that cash collected from the sale of drugs was taken to a bureau de change at the border, where large sums of money in small denominations were exchanged into denominations of a foreign currency. This money was then moved in bags of cash across the border and abroad to purchase a further supply of drugs.

Further investigation identified a scheme in which illegally obtained funds were deposited under a false name into a holding account within the bureau de change, which was controlled by the money launderer. During a search of the premises, it was also established that the bureau de change did not maintain detailed records of cash transactions.

Three individuals were charged with money laundering in this investigation.

Key Message

Although the bureau de change had an obligation to identify customers and maintain records, it did not do so. A money laundering operation was uncovered through the police investigation; however, this example shows that, if preventive measures are not enforced, laundering activity can continue, even in supposedly regulated financial institutions.



Case Study 11

Payments structured to avoid detection

Over a four year period, Mr. A and his uncle operated a money remittance service known as Company S and conducted their business as an agent of a larger money remitting business that was suspected of being used to finance terrorism. Later, an investigation was initiated in relation to Company S based on a suspicious transaction report.

The investigation showed that over the four year period, Mr. A's business had received over US\$4 million in cash from individuals wishing to transmit money to various countries. When Mr. A's business received the cash from customers, it was deposited into multiple accounts at various branches of banks in country X. In order to avoid reporting requirements in place in Country X, Mr. A and others always deposited the cash with the banks in sums of less than US\$10,000, sometimes making multiple deposits of less than US\$10,000 in a single day.

Mr. A was charged and pleaded guilty to a conspiracy to "structure" currency transactions in order to evade the financial reporting requirements.

Key Message

This case underlines the need to have mechanisms in place to monitor and link transactions (especially cash deposits) made by the same individual or entity through different branches of the same bank, or through different banks.

Case Study 12

Cross border cash

Three suspicious transaction reports were received, relating to a number of transactions which were carried out at Danish banks, whereby large amounts of money were deposited into accounts and then withdrawn shortly afterwards as cash. The first report concerned an account held by customer X. Upon initial investigation, the subjects of the reports (X, Y and Z) were not known in police databases as being connected to drugs or any other criminal activity. However, further investigation showed that X had imported more than three tonnes of hashish into Denmark over a nine-year period. Y had assisted him on one occasion, whilst Z had assisted in laundering the money.

Most of the money was transported by Z as cash from Denmark to Luxembourg



where X and Z held 16 accounts at different banks, or to Spain and subsequently Gibraltar, where they held 25 accounts. The receipts from the Danish banks for the withdrawn money were used as documentation to prove the legal origin of the money when the money was deposited into banks in Gibraltar and Luxembourg. It turned out that sometimes the same receipt was used at several banks, so that more cash could be deposited as "legal" than had actually been through the Danish bank accounts.

X and Y were arrested, prosecuted and convicted for drug trafficking offences and received sentences of six and two years imprisonment respectively. A confiscation order for the equivalent of US\$6mn was made against X. Z was convicted of drug money laundering involving US\$1.3mn, and was sentenced to 21 months' imprisonment.

Key Message

Financial institutions should not accept proof of deposit to a bank account as being equivalent to proof of a legitimate origin. Carrying illegal proceeds as cash across national borders remains an important method of money laundering.

Case Study 13

Bureaux de change

At the point when exchange offices became regulated, and it became subject to obligations to prevent money laundering, one bureau ("The Counter") had been doing business in a small town near the German border for a number of years. The Counter often had a surplus of bank notes with a high denomination, and the owner (Peter) knew that these notes were not popular and so exchanged them into smaller denomination notes at a nearby bank. Prior to the new legislation taking effect, persons acting on behalf of The Counter regularly exchanged amounts in excess of the equivalent to US\$50,000, but immediately after the legislation took effect, the transactions were reduced to amounts between US\$15,000 and US\$30,000 per transaction. The employees of the bank branch soon noticed the dubious nature of the exchanges did not have any sound economic reason, and the transactions were reported.

Peter had a record with the police relating to fencing and dealing in soft drugs, and because of this he transferred the ownership of The Counter to a new owner with no police record (Andre). Andre applied to register The Counter to the



Central Bank as an exchange office and was accepted on a temporary basis. The financial intelligence unit consulted various police files and established that the police had been observing this exchange office for some time. The suspect's transactions were passed on to the crime squad in the town where The Counter has its office, and it started an investigation. A few months later, the crime squad arrested Andre, house searches are made, expensive objects and an amount equivalent to more than US\$250,000 in cash were seized. The records of The Counter showed that many transactions were kept out of its official books and records. For example, over a period of thirteen months The Counter changed the equivalent of more than US\$50mn at a foreign bank without registering these exchange transactions in its official books and records. The investigation showed that The Counter and its owners were working with a group of drug traffickers, who used the exchange office to launder their proceeds, and this formed a substantial part of the turnover of the business.

The drug traffickers were prosecuted and convicted and are now serving long prison sentences. Andre was sentenced to six years in prison for laundering the proceeds of crime and forgery. Peter moved abroad with his family. A separate legal action is still pending to take away Andre's profits, the confiscated objects and the cash found. The Counter has been closed and its registration as an exchange office rescinded.

Key Message

This case shows the need for banks and large, legitimate bureaux de change to pay attention to their business relations with smaller bureaux, particularly when supplying or exchanging currency with them.

Case Study 14

Alternative remittance systems use of retail outlets

This case involved a number of overseas remittance services. Common elements of these services were that they operated from retail shops selling clothes or fabrics and arranged the transfer of money to Country A (for a fee).

The largest remittance service among those investigated, 'Servicio Uno', was an incorporated company and had an annual turnover in excess of US\$3.3mn. It accepted money from individual customers and also received funds from smaller remittance services locally and regionally. These smaller services channelled

money through Servicio Uno because it had an extensive family-based delivery network in Country A.

The general method used by Servicio Uno was as follows-

Cash was received from customers and sub-agents; a proportion of these funds was deposited in a bank, and some was kept on hand.

Funds were transferred to Country A in two ways: either by telegraphic transfer purchased with cash or cheque; or by sending money to a trading company, 'Trans-Expedición SA', in Country B. This second company did business in Country A and had associates there that owed it money. Once Trans-Expedición received the money in Country B from Servicio Uno, it advised its debtors in Country A to pay a specified amount direct to another remittance business, Remesas-X, in Country A.

Twice weekly, Servicio Uno faxed a list of required deliveries to a company it owned and operated in Country A, including details of the sender, the recipient and their address, and the amount and type of currency or gold bars to be delivered. A fee of 5-10% was charged by Servicio Uno.

There was also evidence of substantial amounts of money flowing from Country A back to Servicio Uno. A fax was sent from Country A to Servicio Uno instructing it to provide a specific amount of money to an individual in Servicio Unos country or to pay the funds into a particular bank account there. No funds were actually transferred from Country A. Instead, a method was used whereby the remittance services at either end of the operation paid off each others liability with their own assets.

Investigations revealed that several legitimate businesses in Servicio Uno's country had also repatriated funds to Country A using this method. They also revealed that a previously convicted money launderer had on at least one occasion transferred US\$60,000 to Country A through Servicio Uno. Additionally, one sub-agent of Servicio Uno transferred funds on behalf of two active drug traffickers.

Key Message

This is a classic example of an alternative remittance system. The difficulties that an investigative agency might have if it were to detect part of the scheme would be the ability to determine the links to and from the third country. The process would be further complicated by the high volume of legitimate business



using this channel to move funds, and by the indirect settlement methods sometimes employed.

Case Study 15

Alternative remittance systems laundering cash from the sale of narcotics

Cash from the sale of narcotics was brought to shops and bureaux de change (controlled by a single organisation) in a town located in an overseas territory of Country P. The shops provided specially validated coupons in return for the deposits. These coupons were then used as bearer instruments that permitted the holder to obtain funds to purchase more drugs or to make investments. The controlling organisation also owned several real estate agencies.

The laundering network converted currency from other countries through middlemen that were paid a commission for the use of their identities in the depositing of these currencies at financial institutions. An employee at one of these institutions was also involved in the scheme. Other funds processed through this system originated in the local black market in consumer goods intended for smuggling operations into the neighbouring jurisdiction.

The law enforcement investigation of this case brought about charges against 73 persons, and the seizure of 10 tonnes of narcotics, 11 boats and US\$4.7mn in foreign currency. Suspicious transactions submitted by local financial institutions during the scheme reported transactions totalling more than US\$400mn.

Key Message

This scheme is yet another example of an alternative remittance scheme, but one in which coupons were issued to evidence the deposit of cash proceeds.

Case Study 16

Alternative remittance systems - supported by import/export activity

A national from Country S was arrested in Country M on suspicion of unlicensed banking. The investigation revealed that this subject had been running an informal fund transfer system (hawala) for almost four years. Three other individuals who had already left country M were also identified as associates.

Balances were settled between countries M and S through import/export transactions relating to car parts. A company exported car parts from Country M



to an importer in Country S with a specific charge. The importer from country S paid 50% of the specific charge directly to the exporter in country M and the hawala operators paid the other half. In return, the importer in Country S paid 50 % of the price to the groups account in country S to settle the balance. The payment was made in local currency and at a rate advantageous to the receivers, so that the group was certain to make a given profit from the transaction.

Key Message

Had the exporter's bank been alert to the source of funds for payment of the exported goods, suspicions would have been raised that payment was being made from two different sources in respect of one transaction.

Case Study 17

Underground banking activity revealed through large turnover in small business

Investigations were triggered by several reports of suspected money laundering submitted by various banks over a period of three years in respect of a national of Country N born in south Asia. Although the suspect ran a small business with an annual turnover of around US\$150,000, between US\$1.7mn and 3.5 mn per year flowed through his private accounts.

Investigations revealed that the suspects business was the headquarters in Country N of an international underground bank with branches in several Central Asian and European countries and a chain of 14 branches in Country N. In addition to being used by Asian nationals to transfer small amounts to support their families back home - a traditional use of the hawala system - this illegal banking system was used to transfer considerable sums for human trafficking into Europe.

The suspect and the manager of one branch were arrested. A number of properties were searched throughout Country N. A forfeiture notice amounting to approximately US\$350,000 was issued against the suspect and around US\$140,000 in cash was confiscated in preparation for forfeiture. The suspect and the manager were sentenced for human trafficking and the accused voluntarily renounced his claim to the confiscated cash.



Key Message

This is a classic case where KYC information relating to the size of the business activities of the account holder demonstrated that the legitimate business activity could not possibly generate the funds available to the owner of the business.

Case Study 18

The derivatives market: a typology

In the following example of how funds could be laundered using the derivatives market, the broker must be willing to allocate genuinely losing trades to the account in which criminal proceeds are deposited. Instead of relying on misleading or false documentation, the broker allocates genuine loss-making documentation to the detriment of the 'dirty money' account holder.

As an example, a broker uses two accounts, one called 'A' into which the client regularly deposits money which needs laundering, and one called 'B' which is intended to receive the laundered funds. The broker enters the trading market and 'goes long' (purchases) 100 derivative contracts of a commodity, trading at an offer price of \$85.02, with a tick size of \$25. At the same time he 'goes short' (sells) 100 contracts of the same commodity at the bid price of \$85.00. At that moment, he has two legitimate contracts which have been cleared through the floor of the exchange.

Later in the trading day, the contract price has altered to \$84.72 bid and \$84.74 offered. The broker returns to the market, closing both open positions at the prevailing prices. Now, the broker, in his own books assigns the original purchase at \$85.02 and the subsequent sale at \$84.72 to account A. The percentage difference between the two prices is 30 points or ticks (the difference between \$84.72 and \$85.02). To calculate the loss on this contract, the tick size of \$25 is multiplied by the number of contracts, 100, multiplied by the price movement, 30. Thus: $\$25 \times 100 \times 30 = \$75,000$ (loss).

The other trades are allocated to the B account, which following the same calculation theory results in a profit as follows: $\$25 \times 100 \times 26 = \$65,000$ (profit). The account containing the money to be laundered has just paid out \$75,000 for the privilege of receiving a profit of \$65,000 on the other side. In other words, the launderer has paid \$10,000 for the privilege of successfully laundering \$75,000. Such a sum is well within the premium professional launderers are prepared to pay for the privilege of cleaning up such money. As a transaction, it is perfectly lawful from the point of view of the broker. He has not taken the



risk of creating false documentation, which could conceivably be discovered, and everything has been done in full sight of the market.

Case Study 19

Criminal cash proceeds placed through margin trading

This case involved the theft of approximately US\$384mn from a bank in country T over a ten-year period. Initial investigations revealed that the money was sent to country G and laundered through a series of 550 bank accounts in the names of 80 companies. Much of the money was invested in the property and stock markets in Country G and ultimately used at will by the four principal thieves. At one time during the fraud, one of the thieves was reported as being the largest margin stock investor in the Country G market, with a huge turnover in stocks and shares through some of Country G companies, as well as enjoying dividends from long term investments. Initial investigations appear to indicate that the majority of funds stolen in Country T occurred towards the end of the ten-year period, when a regional economic downturn adversely affected the local property and stock markets.

No disclosures were ever made by stockbrokers about the dealings of these companies. Four people were charged with money laundering and warrants were issued for a number of others.

Case Study 20

Shell corporations

A drug trafficker used his proceeds to purchase a property, in respect of which part was paid in cash and the remainder was obtained through a mortgage. He then sold the property to a shell corporation, which he controlled, for a nominal sum. The corporation sold the property to an innocent third party for the original purchase price. By this means the drug trafficker concealed his proceeds of crime in a shell corporation, and thereby attempted to disguise the origin of the original purchase funds.

The accused pleaded guilty and an order of forfeiture was granted. The property, which was part of the money laundering scheme, was disposed of by the authorities.



Key Message

This case illustrates the need to trace the ownership history of a property carefully, in order to identify possible links between owners, and any suspicious transfers that may indicate attempts to co-mingle assets. There is also a need for law enforcement agencies to be familiar with the general rules and practice regarding the purchase of property in relevant jurisdictions, and the need to be aware that transfers involving nominal amounts can be easily structured in some jurisdictions.

Case Study 21

Shell companies and Corporate Service Providers

During a two-year period, financial institutions in a European country made suspicious transaction reports to the relevant financial intelligence unit. The reports identified large cash deposits made to the banks, which were exchanged for bank drafts made payable to a shell corporation based and operated from an Asian jurisdiction. The reports identified transfers totally approximately US\$1.6mn to an account held by the shell corporation at a financial institution in the Asian jurisdiction.

At the same time, police had been investigating a group in that country which was involved in importing drugs. The following year, police arrested several persons in the group, including the principal, who controlled the company in the Asian jurisdiction. They were charged with conspiring to import a large amount of cannabis. A financial investigation showed that the principal had made sizeable profits, and a large percentage of this was traced and restrained. A total of approximately US\$2mn was sent from the European country to the Asian jurisdiction, and subsequently transferred back to bank accounts in Europe, where it was restrained.

Two methods were used to launder the money. The principal purchased a shell company in the Asian jurisdiction, which was operated there, by a secretarial company on his instruction. The shell company opened a bank account, which was used to receive cashiers' orders and bank drafts, which had been purchased for, cash in the country of origin. The principal was also assisted by another person who controlled (through the same secretarial company) several companies, which were operated for both legitimate reasons and otherwise. This person laundered part of the proceeds by selling the funds on to several other jurisdictions, and used non face-to-face banking (computer instructions from the original country) to do so.



Seven persons including the principal were put on trial in the European country on charges of drug trafficking, and the principal and three other persons faced money laundering charges.

Key Message

This example shows how attractive and easy it is for criminals (even if not part of international organised crime) to use corporate entities in other jurisdictions, and to transfer illegal proceeds through several other jurisdictions in the hope of disguising the origin of the money.

It demonstrates the ease with which company incorporation services can be obtained, and shows that many of the companies, which sell shell companies, as well as the secretarial companies, which operate them, are not likely to be concerned about the purpose for which the shell company is used.

It highlights the need for financial institutions to have a system, which identifies suspicious transactions not just at the front counter, but also for non face-to-face transactions, such as occurred in this case.

It can take some time to conduct international financial investigations and to trace the proceeds of crime transferred through several jurisdictions, and there is a consequent risk that, during the investigation, funds will be dissipated.

Case Study 22

Front companies, insurance and bureaux de change

An FIU received a suspicious transaction report from a life assurance company. The report referred to Mr. H, born and resident in a Latin American country, as having recently taken out two single premium life insurance policies for a total amount of US\$702,800. Subsequent information provided to the FIU indicated that the policies' premiums had been paid with two personal cheques made out by a third party and drawn against a major bank. The third party, Mr. K, was also resident in the same Latin American country, although he was not a national of that country. Further checks at Mr. K's bank revealed that both he and Mr. H had signature authority on two business accounts, Sam Ltd and Dim Ltd.

Examination of the accounts showed that transactions, especially in Mr. K's account, were carried out on behalf of Mr. H. Thus, the account had received funds from abroad and had also been used for other financial products besides the life insurance policies. Indeed, ten cheques in US dollars, totalling



US\$1,054,200, drawn against American banks and issued by two bureaux de change operating out of the Latin American country where the two men resided, had been deposited into Mr. Ks account.

This activity appeared to show that the funds had been used to pay the insurance premiums on Mr. H's life and to acquire stakes in investment funds (also for Mr. H) amounting to another US\$210,840. There were also other related transactions in the accounts of the two companies and Mr. H's personal account. Cash or cheque transactions for amounts between US\$14,000 and US\$70,000 were among the related transactions. In one instance, a cheque was drawn on the Sam Ltd account for US\$63,300 on the day following the deposit of US\$70,280 in cheques into Mr. Ks account.

Checks into the backgrounds of Mr. H and Mr. K revealed that Mr. H was suspected of being involved in cocaine trafficking in Latin America. Mr. K had some minor violations (uttering bad cheques etc.); however, he had no serious criminal background. The business activities and backgrounds of Sam Ltd and Dim Ltd were looked at. In each instance, the companies had been incorporated with a stock capital of US\$36,400 in which Mr. H and Mr. K had a 50% interest and were joint directors. Queries made at the "Balance of Payments Office" as to foreign collection and payment, revealed a total absence of operations in the previous two financial years.

It appeared that Mr. K was being used as the front man for Mr. H's efforts to move funds out of his country of residence. For greater security of the scheme, firms under their control, that did not perform any corporate or commercial activity, were established. Mr. H received the funds deposited into Mr. K's account through the single premium insurance policies and shares in investment funds that had been paid for by that account, as well as through indirect income from the companies mentioned. In this case, the FIU believed there to be sufficient signs of money laundering and therefore passed the matter on to prosecutorial authorities.

Key Message

This operation shows that payment instruments or third party involvement, having no apparent economic relationship to the transaction, are often a key indicator of suspicious activity. It is worth noting that, so as to minimise suspicion, Mr K was obviously selected based on his lack of prior criminal record and his nationality.

The activities of the front companies were also conducted in such a way as to give the appearance of transactions from corporate activities. The case also highlights the potential value of suspicious transaction reporting by insurance companies.

Case Study 23

Front companies

An FIU in Country B received a report of a series of suspicious transactions involving the bank accounts of a West African citizen and his businesses, which specialised in industrial fishing. These accounts were opened in banks located in Country B and consisted primarily of money changing operations. The businessman also owned several residences in his home country and in the capital region of Country B. The companies that he jointly managed all had the same address in his home country.

The personal account of the West African businessman received a number of transfers from accounts in another European country and in his home country (over US\$2 million in a two-year period). The companies' accounts received transfers from several business entities based in Europe, ostensibly linked to fishing related activities (over US\$7 million over a three-year period). The transfers out of the account (estimated at nearly US\$4 million over the same period) were made to various companies whose business was (according to official records) connected with maritime activity and to other individuals.

The FIU analysis showed that the income of the West African companies concerned was grossly disproportionate to reported sales. In fact, the account transactions seemed to have little to do with industrial fishing (i.e. foreign currency sales, transfers from the bank accounts of European residents, transfers between the personal account of the West African businessman and his businesses, transfers between these businesses and those of Europe-based partners).

Furthermore, according to additional information received by the FIU, one of the business partners of the West African businessman, a co-manager of one of the companies, was suspected of being involved in several financial offences in Italy. This individual reportedly had close associations with two Italian organised crime figures, and his Italian businesses have become the target of an investigation into money laundering in that country. Still another business partner of the West African businessman appeared also to be involved in financial and fiscal offences.



Key Message

Given the unusual account transactions and the lack of a clear economic purpose or connection for some of the business activities, the operations described in this example very likely constitute a money laundering scheme to conceal the illegal sources of proceeds derived from various criminal activities. This case gives further support to the need for analysis of information from a variety of sources (suspicious transaction reports, financial institutions, company registries, police records etc.) in order to gain a full picture of a complex laundering scheme.

Case Study 24

Silver and gold smuggling

Cross-jurisdictional investigations permitted the detection of a silver and gold smuggling system aimed at VAT evasion and the laundering of the illicit profits of several local, regional and global criminal organisations. The banking and financial systems were used to process large-value transactions supporting the fictitious payment of precious metals supplies. The laundering was primarily undertaken through:

Creation of a network of companies, including financial, throughout the region, with the task of "filtering" the money. Using criminal proceeds derived from cigarette smuggling, drug trafficking, illegal arms trafficking and the smuggling of oil products, to purchase silver and gold, which was in turn smuggled into the markets of Country J and other European countries. Reinvestment of the profits of the illicit trafficking of silver into smuggling activities. Use of false invoices in respect of the importation of precious metals which never actually reached country J. Use of bearer savings deposit passbooks and of false Treasury certificates of deposit to be offered as guarantees to the banks for the purchase of precious metals.

Fifteen suspects were arrested for criminal conspiracy aimed at money laundering and smuggling, and four suspects were charged with money laundering offences. The total amount of funds involved was US\$101mn with the consequent evasion of export duties amounting to US\$72mn, VAT evasion totalling US\$37mn and the laundering of over US\$31mn.

Key Message

Enquiries should always be undertaken to ascertain the purpose and beneficial

ownership of companies that are formed in offshore jurisdictions with lax corporate registration requirements. The source of the economic activity that created the funds for transfer should be established. Where the sale of precious metals is involved, checks should be made that the goods exist and that excise duty and VAT has been paid.

Case Study 25

Laundering the proceeds of fraud through the diamond market

A known criminal who had benefited financially from a fraud in an overseas jurisdiction attempted to transfer US\$8.2mn to a jeweler in Country A with a view to purchasing precious stones. The bankers in Country A had already submitted various suspicion reports in relation to the individual, and on this occasion the bank made a further suspicion report and took the commercial decision to freeze the account. On investigation, it was determined that the objective of purchasing the precious stones had been an attempt to launder the proceeds of the fraud.

Key Message

Suspicious transactions reports will not always bring immediate results and where a series of suspicion reports has been made justifying significant concern, it may be necessary to freeze the account voluntarily, pending an investigation. Confidential discussions with the local FIU will normally confirm when a criminal who is known to the FIU is involved.

Case Study 26

Terrorists collect funds from lawful sources

A number of individuals known to belong to religious extremist groups established in the south-east of Country C (a FATF country) convinced wealthy foreign nationals, living for unspecified reasons in Country C, to finance the construction of a place of worship. These wealthy individuals were suspected of assisting in the concealment of part of the activities of a terrorist group.

It was later established that S, a businessman in the building sector, had bought the building intended to house the place of worship and had renovated it using funds from one of his companies. He then transferred the ownership of this building, for a large profit, to Group Y belonging to the wealthy foreigners mentioned above. This place of worship, intended for the local community, in



fact also served as a place to lodge clandestine "travellers" from extremist circles and to collect funds.

Soon after the work was completed, it was noticed that the place of worship was receiving large donations (millions of dollars) from other wealthy foreign businessmen. Moreover, a Group Y worker was said to have convinced his employers that a "foundation" would be more suitable for collecting and using large funds without attracting the attention of the local authorities. A foundation was thus reportedly established for this purpose.

It was also believed that part of S's activities in heading a multipurpose international financial network (for which investments allegedly stood at US\$53mn for Country C in one particular year alone) was to provide support to a terrorist network. S had made a number of trips to Afghanistan and the United States. Amongst his assets were several companies registered in Country C and elsewhere. One of these companies, located in the capital of Country C, was allegedly a platform for collecting funds. S also purchased several buildings in the south of Country C with the potential collusion of a notary and a financial institution.

When the authorities of Country C blocked a property transaction on the basis of the foreign investment regulations, the financial institutions director stepped in to support his clients transaction and the notary presented a purchase document for the building, thus ensuring that the relevant authorisation was delivered. The company's funds held by the bank were then transferred to another account in a bank in an NCCT jurisdiction to conceal their origin when they were ultimately used in Country C.

Even though a formal link was not able to be incontrovertibly established between the (more or less) legal activities of the various parties in Country C and abroad and the financing of terrorist activities carried out under the authority of a specific terrorist network, the investigators suspect that at least part of the proceeds from these activities have been used for this purpose.

Key Message

The scale and complexity of the corporate and business arrangements, and the amounts involved, should not deter proper checks and monitoring.



Case Study 27

Simple transactions found to be suspect

The financial intelligence unit (FIU) of Country E forwarded to the judicial authorities ten files in relation to money laundering derived from terrorism. In general, the files dealt with instances in which simple operations had been performed (retail foreign exchange operations and international transfer of funds), revealing links with other countries. Some of the customers had criminal records, particularly for trafficking in narcotics and weapons, and were linked with foreign terrorist groups.

In one of the files submitted by the FIU in relation with terrorism, the customer was the holder of a current account and of a savings account with the reporting financial institution. Moreover, he purchased securities, and a single premium life insurance contract, in the same institution. He executed several transfers from his current account to beneficiaries in different countries. The suspicions of the bank arose from the fact that a name similar to that of the customer appeared on the consolidated list of persons and/or entities included in the UN Security Council Committee on Afghanistan (S/RES/1333(2000)) and Regulation 1354/2001 of the European Commission).

The suspicion of the bank was strengthened by the fact that the customer had been progressively withdrawing funds he held at this bank since the end of April 2001. He successively cleared out his savings account, sold the securities he had purchased (before their maturity date), surrendered his life insurance policy and finally transferred his remaining funds to the European country where he resided. The last operation he performed occurred at the end of August 2001, that is, about two weeks before the attacks in the United States on September 11th 2001.

The bank has had no more contact with this customer since August 2001.

Key Message

Timely identification and reporting of suspicions matters by firms is important, even if the authorities are not able to react effectively and in good time.



Case Study 28

Charity used to finance terrorism

One UK investigation arose as a consequence of a suspicious transaction report. A bank disclosed that an individual who allegedly was earning a salary of £12,000 per annum had a turnover in the account of £250,000. A financial investigation revealed that the individual did not exist and that the account, fraudulently obtained, was linked to a Middle East charity. A fraud was being perpetrated for the purpose of raising funds for a terrorist organisation. Donations were paid into an account and the additional charitable payment was being claimed back from the government. The donation was then returned to the donor. This fraud resulted in over £800,000 being fraudulently obtained.

Key Message

Even UK charities can be used to raise funds for terrorist purposes.

Case Study 29

Correspondent banking, wire transfers facilitate transactions by shell companies

Company Q, a suspected shell company registered in Country F (a FATF member country), was reportedly involved in the transportation of oil and other raw materials (metal, timber, gas). Company Q was a customer of a bank in Country G that maintained a correspondent account at a Country F bank. The Company received several wire transfers from another, rather vague company located offshore. At the request of the bank in Country F, the Country G bank asked Company Q to provide copies of a business contract that would justify the financial activity. The Country F bank submitted an STR in respect of these transactions.

Rather than providing the requested documents to the bank, Company Q simply closed its account.

Key Message

Sometimes there is a need to look through the correspondent. Due diligence can reveal situations shown by this case that warrant reporting to the relevant authorities.



Case Study 30

Private banker helps conceal suspect's illegal proceeds

This example relates to a bank whose services included institutional brokering, retail brokering, private client services, global equity derivatives, securities, futures and margin lending. Clients of the bank could enter into a private client agreement, which enabled the client to perform transactions by telephone or facsimile. During the course of an investigation, difficulty was encountered in matching money coming into the suspects trust account with funds sent out of the country by a co-offender. Upon reconstructing the money trail through bank deposit and withdrawal records, it was found that the co-offender had sent an equivalent amount of funds out of the country through international telegraphic transfers but the transfer documentation did not record the co-offender as the ordering customer - who was shown as the merchant bank.

This provided a way to disguise the remittance of funds offshore.

Key Message

Inadequate transaction records can preclude "matching up" of connected transactions that, when matched, can lead to suspicion.

Case Study 31

A bank observes large value cash transactions executed through its accounts almost on a daily basis by a trading concern, X Enterprises. The deposits are always below the reporting threshold of Rs. 10 lakh. These deposits are done using multiple tellers at the same branch. The value of each cash transaction hovers between Rs. 8 to 9.5 lakhs. The customer is in the business of garments. The pattern observed is deposit of cash followed by simultaneous transfer to other accounts within the bank or issue of cheques. On investigation into the profile of other accounts it is observed that these accounts are of entities of varied industries like chemicals, plastic, metals, food grains & packaging. The turnover in each of these accounts amounts to crores of Rupees. On scrutiny it is observed that many of these entities are related by virtue of same partners, same address, same telephone. They have different PAN numbers. Most of these entities are in near vicinity of each other. These entities have availed no credit facilities from the banks.



The Branch manager decides to visit some of these entities and discretely finds that none of these entities have infrastructure to support the activities as per their profile. Many are not open during business hours. It is found that these entities are into business of converting cash into cheques and vice versa for persons across a spectrum of businesses. This type of business is colloquially called 'entry business'. An STR is raised for these accounts.

Key Message:

This is a classic example of money laundering in Indian Context. Enhanced Due diligence helped reveal that transactions are not in line with the profile of the customer and indeed suspicious.

Case Study 32

The branch manager comes across a large value transaction for purchase of property in Mr. A's savings account worth Rs. 30 crores in month of October. A closer analysis of the account statement for last 3 months reveals about 50 transfer transactions from 10 different accounts in names of customers having similar or different family names. On further perusing through account statements of these customers, it is observed that cash has been deposited therein and this is followed by transfer to Mr. A's Account. The Branch manager also finds that all these accounts were opened on same day. An STR is filed for these accounts.

Key Message:

While analyzing the trigger for an unusual transaction one should examine transactions, which precede as well as following the unusual transactions. This may enable the Bank to confirm suspicion.

Case Study 33

Mr. B is a wealthy customer staying in a plush locality New Delhi. The branch manager observes that on a particular day in February the turnover in his account crosses 25 transactions. On analyzing the account for the day it is observed that the customer has deposited 20 demand drafts of Rs 45,000 each. Customer refuses to divulge the reason for these transactions and hurriedly hangs up the telephone. On a closer look at account statement an account transfer is seen in January to his wife's account. On analyzing the account of the spouse of the customer, similar pattern in the month of January is observed. An STR is filed for these accounts.

Key Message:

Analysis of linked accounts help a bank to determine nature of customer activity.

Case Study 34

A Bank officer processing foreign currency cheques observes that an Non Resident customer receives three to four foreign currency cheques in a day for clearing. There are also credits from on line site aggregators. Each credit is between 3000 to 4000 USD. These credits come from different countries. On checking with the customer's mandate holder, he states that these are payments received by way of commission in the business of internet marketing. On conducting a search over the internet it is also revealed that the customer is running a site which invites people to subscribe to his services. The content of the site is perfectly educational and legal. However this conflicts with the version of the mandate holder. The customer has not made a single withdrawal from the account over a period of one year that he has an account with the bank and the total balance in the account is very high. An STR is filed for the customer.

Key Message:

In respect of certain customers a desktop due diligence in form of Internet searches may reveal details of the customer activity and help gather evidence for reporting a suspicious transaction.

Case Study 35

An NRI customer from Europe receives remittances worth crores of Rupees into his account. The proceeds are invested into various capital market instruments covering mutual funds, shares and securities. On checking the remitter details it is observed that funds are being received from his account in Europe. The bank officer checks the remittances received from this remitter across the Bank and finds that similar large value amounts are transferred into accounts of un related persons over last six months whose accounts have since gone dormant. The amount has been withdrawn in cash and currently there is no balance in these accounts. These accounts are reported as an STR

Key Message:

While an instant unusual transaction may not appear to be suspicious, related accounts may throw up suspicion. Therefore it is necessary to look at the totality of the customer transactions.



Case Study 36

The account of a resident Y is receiving a number transfers from a non-resident X stationed in gulf through internet transfers. The account of X in turn is receiving remittances from another non resident Z working in same oil refinery as X. Z receives money through large value clearing cheques from another non resident W. In spite of due diligence it is not possible to establish any relation between these persons. The manager files the STR and two months later finds the name of the Y as being involved in a terrorist act in a foreign country. An STR is filed in the case.

Key Message:

Look out for transactions that do not make economic sense.

Case Study 37

The Branch manager during his analysis of AML exception reports for May finds some accounts where cash is being deposited through multiple branches and withdrawn on same day. One such account holder is Mr Y. who ensures that he does not maintain balance over a period of one or two days. Deposits are in form of third party walk ins. The amounts deposited are between Rs 2500 to 3000. The manager directs the teller to inform him the next time any person other than the account holder approaches to deposit cash in the account. Five days later the manager is alerted by teller and immediately asks the depositor reason for depositing cash in this account who informs him that he has been instructed to do so by one Mr T who has promised him a lottery winning of Rs 10 lakhs provided he deposits Rs 3000 as processing fee. Manager immediately files an STR for same.

Manager comes across another such account in name of Mr. O. Unlike Mr. T the amounts are received by him through ATM cash deposits. No person physically visits branch to deposit the amount. The transaction pattern is similar to that of account of Mr. Y. An STR is filed by the manager. One month later the manager receives a letter from the Narcotic Control Bureau asking him further information in relation to Mr. O. It has now come to light that O was a drug peddler was using bank's channels to receive cash from his customers who were couriered drugs.

Key Message:

Compare the activity in the account to the profile of the customer/behavior of such segment of customers. This may reveal unusual behavior.

**Case Study 38**

Mr. D is holding a credit card of the bank with a Rs 1 Lakh limit. He deposits large value of cash to repay his card dues. His spends are on all airline company web sites. The total value of spends per month is approximately 15 lakhs. All repayments are made in cash. On investigation into the KYC documents it is observed that he is working in a travel agency. It can thus be deduced that he takes cash from customers and uses his credit card to book tickets from them and repays same into his card account after one month.

Key Message:

Misuse of personal banking channels /products for business purposes.

Case Study 39

A person spends approximately five lakhs every month on his credit card. The spends are on only one particular merchant establishment. On closer analysis the merchant establishment is a on line gambling site in a foreign country. It is suspected that the customer may be transferring value by way of credits into account of some other person holding account with the site.

Key Message:

Misuse of banking channels for illegal purposes should be reported as suspicious transaction.

Case Study 40

A savings account of Mr. ABC (a telephone booth operator) is held with a banks branch in a small town for about one year. It is observed that in recent times persons other than the depositors or his family members frequent the branch for making withdrawals. The teller informs the branch manager about this unusual activity. On checking with the customer discretely he informs that he has allowed certain persons to use his account for conducting transactions. The Branch manager immediately reports this as a STR.

Key Message:

Inputs from branch are helpful in determining suspicious transactions



Case Study 41

A friendly customer having a savings bank account asks the cashier at the branch as to what the bank would do if he deposits Rs. 2 crore in cash from him. The total turnover in the customer's account has thus far been in range of Rs. 3 lakhs in a year. However the customer never carries out this transaction. The branch files a STR in the matter for an attempted suspicious activity.

Key Message:

Although the transaction has not taken place as required by RBI regulations attempted suspicious transactions should also be reported.

Case Study 42

M/s. ABC Electronics P Ltd, a new customer lodges an export bill for collection with the Bank. The customer has submitted an invoice and bill of lading worth \$ 20,00,000 for sale of 300 laptops. The invoice is raised on M/s PQR trading, Nigeria. The Bank Officer on scrutiny of the bill finds that the value of a laptop as per this invoice is highly overvalued and files an STR for the same. On investigation it is revealed that M/s PQR, the front for a criminal wanted to send an amount of \$ 10,00,000 to India. M/s ABC electronics P Ltd was a front for the hawala operator who through over invoicing achieved this through the official channel.

Key Message:

Transactions that do not make economic sense should be identified for reporting suspicious transactions.

**Annexure F****Suggested solutions to certain situations****Situation 1**

ABC Enterprises has a current account with you. ABC Enterprises is a dealer of house hold appliances. Normal transactions in the account are daily cash deposits of about INR 100,000 and deposit of cheque and credit card charge slips for about 100,000. Payments to various distributors are through cheques. There are some cash withdrawals especially in the beginning of the month for salary payments. During the last 15 days, you have noticed that the cash deposits are in the range of INR 150,000 to INR 200,000 and there have been some increase in the deposits by cheques and charge slips as well.

Solution

Mere increase in the cash deposit does not necessarily mean a suspicious activity. Here in this case, there has been an increase in the cheque/ charge slips deposit as well. There could be some reason for the increase in sale, like a festival season. Make enquiry about a reason for the increased sale and also check the payment part to see whether the money is going anywhere other than the usual suppliers. File a SAR only if you are not convinced about the reason for the increase in cash deposit.

Situation 2

DEF Traders maintains a current account with you for the last three months. The account was opened with a deposit of INR 25,000. While opening the account, the business declared is Commission agents and he mentioned that he is getting distribution agency for some well-known cosmetic and detergent products. The expected transaction volume declared was monthly credit of INR 1 million and an average balance of INR 50,000. There were no transactions in the account for 2 months. For the last one month, the volume of transactions suddenly increased and at present there is a daily deposit of approximately INR 200K and the average balance is around 25,000. The withdrawals are through pay orders and most of the time favouring different firms and the pay orders are paid in clearing through banks in various cities. You met the customer and enquired about the business and he mentioned that he did not take the distributorship of the cosmetic and detergent products as he did not want to restrict his product range and he is now purchasing from various distributors and supplying to small businesses in the



area and the business was very good. Your enquiry revealed that the customer did not have any separate office or godown and the business address given in the AOF is his residence address.

Solution

Though the explanation of the customer could account for the large cash deposits (sale to small traders) and payments to different firms, absence of any godown or distribution set up give sufficient reasons to suspect the bonafides of the customer. An SAR should be filed.

Situation 3

ABC, a walk in customer approaches you. She wanted to open a savings account with you. On your request, she produced a Voter's ID Card and ration card for identity verification and address verification. While taking further details of activity profile, you realize that the customer would be getting a monthly pension credited to her account and she would be withdrawing most of the amounts for her expenses. You tell her the Bank's rule of maintaining minimum balance in the account and she expresses her inability to do so. Hence, you decline to open the account.

Solution

The refusal to open the account was not due to any suspicion. It was because the customer was not able to meet your banking requirement of maintaining the minimum balance in the account. No SAR to be filed.

Situation 4

LKG Corporation is a SME customer for about 2 years. They are in the import export business and use the bank for their international trades on a regular basis. So far the business had been some export bill collections and some payments against the import documents. They did not have any import LC facility but has an OD facility for INR 2 million. Now the customer has approached you for opening an LC for USD 100,000 for import palm oil. The beneficiary of the LC is in Dubai and the shipment will be made from Malaysia to Mumbai. The customer is offering security of term deposits held in the names of his close relatives.

Solution

We have a fairly good knowledge of the customer. There is nothing apparently suspicious about the transaction on a money laundering point of view.



Situation 5

ABC Enterprises is a partnership firm. The firm opened a current account with your branch in January 2004. The proprietor was identified through his driving license and his address verified through a utility bill. The business address was verified through the agreement with the landlord. Initially there were some cash deposits and cheque deposits and some remittances to Hongkong against import documents, which included Bill of Entry with Customs stamp and invoice. The remittances were small and on all the occasions the goods imported were "halogen lamps". Around June, 2004, the proprietor opened another account in the name of DEF Traders, a partnership firm with him and his wife as partners. He also opened a third account in the name of GHI Agencies, another partnership firm with his wife and another person as the partners. In all these accounts, there have been similar transactions, i.e. deposits through cash and cheques and foreign remittance against the import documents. Of late, the frequency of the transactions increased so much so that the daily deposits in these accounts are just below INR 1 million (There is a reporting requirement for all cash transactions above INR 1million) and the remittances takes place in every three days.

Solution

Definitely, the activities are suspicious. SAR has to be raised.

Situation 6

XYZ Infotech Pvt Ltd. opened an account with your branch about three months back. The company has declared its business as software development. For the first two months there were very few transactions, some low value cash transactions and cheque deposits and withdrawals by clearing. During the last one month, the transactions have increased and there had been some large value inward remittances ranging from USD 25,000 to USD 75,000 and payments by cheques to various firms in different cities in India. Your initial enquiries revealed that the company has its office at the residence of its Managing Director and only have two people working in there. During one of your casual talks with the MD, he mentioned that he had some good contacts abroad and they canvass business and he gets the work done through some of the smaller software companies. You do not feel that most of the beneficiaries of the payments from the account are software companies.

Solution

There are reasons to suspect the activities. The claim of the customer may be true but needs verification through an investigation. SAR should be filed.



Situation 7

MNO Corporation, a partnership firm opened an account with you branch about three months back. AB and his wife are the partners of the firm. AB was working in US as a software engineer and he returned to India recently and started this firm. The declared business of the firm is software development. Initially, there were a few large foreign inward remittances from AB's own account in US and there were payments to various people. These payments could be connected to purchase and development of office premises. During the last one-month, there had been a few large foreign inward remittances and payments to two firms, one in Hyderabad and one in Bangalore. Your casual talks with AB revealed that he has employed about 20 employees in office and as he was not able to cop up with the work he was getting from US, he has sub-contracted the work to two firms, one in Hyderabad and one in Bangalore.

Solution

Though prima facie it appears that the customer is doing a genuine business, it will be prudent to make some enquiries regarding the firms in Hyderabad and Bangalore and an SAR need be raised only if your findings are not conforming to the versions of AB.

Situation 8

FM is one of your savings bank account holder. The account was opened about 5 years ago. As per the KYC profile, FM is working as a journalist for a small newspaper and the transactions in the account had been mostly deposit of salary and withdrawals by cash or cheques in small amounts. For the last three months, he had been receiving foreign inward remittances of approximately USD 5000 from an individual DK in London every month. The customer withdraws the amount in cash in two or three withdrawals. When you enquired with the customer about the purpose of the remittance, he mentioned that he was helping DK in a project regarding tribals in India and the payments are in this respect. He mentioned that he continued to work with the news paper. You do not find any credit for salary in his account for the last few months and a telephone call to the newspaper office confirmed that FM had left the newspaper.

Solution

The transactions are suspicious and should be reported as a SAR.

Situation 9

ABC Charities is a charity trust registered with the charity commissioner. The trust also has necessary government approval for getting donations from abroad



for its charity works. ABC Charities had opened an account with your branch about four years ago with all the necessary documentation. The transactions in the account were mostly cash deposits and cheque deposits for small amounts and there were cash withdrawals mostly to meet the expenses of a home for aged and destitute run by the trust. There were also some foreign inward remittances for amounts varying from USD 50 to USD 100. During the last three months, there had been 10 remittances from one organization from a country that has no strict AML laws or regulations. The amounts of these remittances were between USD 5000 and USD 9000. The total amount received is USD 80,000. Since the starting of these inward remittances, there had been some changes in the withdrawal pattern. Pay orders/demand drafts favouring some individuals and organisations were taken and these were paid through banks situated in locations known for terrorist activity.

Solution

There are enough reasons to suspect the activities. SAR has to be filed.

Situation 10

ABC Corporation is a partnership firm with AB and CD and their wives as partners. About six months ago, ABC Corporation opened a current account with your branch. While opening the account, the firm has shown its business as multi layer marketing and the expected volume of transactions in the account was shown as deposits of INR 2,000,000 and withdrawals of INR 2,000,000. For the first two months of operation, there were very few transactions in the account. Now, there are daily cash deposits of about INR 400,000 through different branches. You have noticed that different people come to the branch for depositing amounts ranging from INR 10,000 to INR 30,000. The withdrawals are by way of clearing cheques or by purchase of demand drafts or pay orders.

Solution

Definitely, the transactions are unusual and need to be investigated. There should be a discreet talk with the customer to clarify as to who are the people who were making deposits to the account and what is the source of these funds. It may also be ascertained as to who are the beneficiaries of the payments from the account. From the explanation, if you get satisfied that the money is from a genuine business and the payments are going for meeting the business related expenses, no SAR be raised. If the customer is evasive or refuses to answer your queries or the explanation does not satisfy you, you have to raise a SAR.



Situation 11

NM has taken a loan of INR 5 million against mortgage of a commercial property valued at INR 20 million. The KYC and credit information collected during the opening of the account showed that NM was a real estate developer and also a trader in commodities. He has declared an average income of INR 3 million during the last three years. He has also been maintaining a current account with you. After six months of taking the loan, NM came with a request to pre-close the loan account. You calculate the amount to be repaid and add the pre-closure penalty and as per the instructions of the customer, transfer the amount from his current account. After about two months, the customer again comes to you and request for a loan of INR 10 million against mortgage of the same property.

Solution

The situation definitely needs further probe. First of all, it has to be seen how the current account was funded for the earlier pre-closure. If these were through cash deposits or other deposits that cannot be connected to his business or personal finance, then you have to file an SAR. If the funding is through genuine business receipts or transparent personal financial transactions, you may seek further clarifications from the customer through normal queries like the purpose of taking the loan, how he intends to repay, etc. and if you are satisfied with the responses, go ahead with the transaction in the usual course of business.

Situation 12

JK is one of your customers. He runs a proprietary firm JK Enterprises. This firm is in transport business, hiring of cars and small trucks. He had taken loans from your bank for purchase of some of the cars and trucks. Within the last two months, he had pre-closed all the loan accounts, one by one.

Solution

The situation is open to suspicion. The important point to be seen is the source of funds to pre-close the account. If the money has come from genuine sources like, loan taken from another financial institution, sale of some assets, etc., then there is no cause for concern but if the source of funds is not clear or suspicious, SAR has to be filed.



ANNEXURE G



RESERVE BANK OF INDIA



(1935-2010)
प्लैटिनम जयंती
PLATINUM JUBILEE

RBI/2009-10/73

DBOD. AML. BC. No. 2/14 .01.001/2009-10

Date: Jul 01, 2009

The Chairman/CEOs of all Scheduled Commercial Banks (excluding RRBs) / all Financial Institutions

Dear Sir,

Master Circular - Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/ Obligation of banks under PMLA, 2002

Please refer to our Master Circular DBOD.AML.BC.No.12/ 14.01.001 / 2008 - 09 dated July 01, 2008 consolidating instructions/guidelines issued to banks till June 30, 2008 on Know Your Customer (KYC) norms /Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002. This Master Circular is a consolidation of the instructions on Know Your Customer (KYC) norms /Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002 issued up to June 30, 2009.

2. The Master Circular has been placed on the RBI website:
(<http://www.rbi.org.in>)

Yours faithfully,

(Vinay Baijal)
Chief General Manager



Master Circular on Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act, (PMLA), 2002

Purpose

Banks were advised to follow certain customer identification procedure for opening of accounts and monitoring transactions of a 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). Detailed guidelines based on the Recommendations of the Financial Action Task Force and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision, with indicative suggestions wherever considered necessary, have been issued. Banks have been advised to ensure that a proper policy framework on 'Know Your Customer' and Anti-Money Laundering measures with the approval of the Board is formulated and put in place.

2. This Master Circular aims at consolidating all the instructions/guidelines issued by RBI on Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Combating Financing of Terrorism (CFT)/Obligations of banks under PMLA, 2002. The Master Circular has been placed on the RBI website (<http://www.rbi.org.in>).

Previous instructions

A list of circulars issued in this regard is given in Annex - III.

Application

- i) The instructions, contained in the master circular, are applicable to all Financial Institutions and all the scheduled commercial banks excluding RRBs.
- ii) These guidelines are issued under Section 35A of the Banking Regulation Act, 1949 and Rule 7 of Prevention of Money-Laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking

Companies, Financial Institutions and Intermediaries) Rules, 2005. Any contravention thereof or non-compliance shall attract penalties under Banking Regulation Act.

- iii) This Master Circular consolidates all the circulars issued on the subject up to June 30, 2009.

Structure

1	Introduction
1.1	KYC/AML/CFT
1.2	Definition of Customer
2	Guidelines
2.1	General
2.2	KYC Policy
2.3	Customer Acceptance Policy
2.4	Customer Identification Procedure
2.5	Customer Identification Requirements - Indicative guidelines
2.6	Small deposit accounts
2.7	Monitoring of transactions
2.8	Closure of Accounts
2.9	Risk Management
2.10	Introduction of new technology - credit/debit/smart/gift card
2.11	Combating Financing of Terrorism
2.12	Correspondent Banking



2.13	Applicability to branches and subsidiaries outside India
2.14	Wire Transfers
2.15	Principal Officer
2.16	Maintenance of records of transactions/Information to be preserved / maintenance and preservation of records / Cash and Suspicious transactions reporting to Financial Intelligence Unit-India (FIU-IND)
2.17	Cash and Suspicious Transaction Report
2.18	Customer Education/Training of Employees/Hiring of Employees
3	Annex
3.1	Annex - I - Indicative List of documents required for opening of accounts
3.2	Annex - II - List of reporting formats
3.3	Annex - III - List of circulars consolidated in the Master Circular

1 Introduction

1.1 Know Your Customer (KYC) Norms/Anti-Money Laundering (AML) Measures/Combating of Financing of Terrorism (CFT)/Obligations of banks under PMLA, 2002.

The objective of KYC/AML/CFT guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable banks to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently.

1.2 Definition of Customer

For the purpose of KYC policy, a 'Customer' 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, and
- any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

2. Guidelines

2.1 General

- i) Banks should keep in mind that the information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Banks should, therefore, ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer should be sought separately with his/her consent and after opening the account.
- ii) Banks should ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travellers' cheques for value of Rupees fifty thousand and above is effected by debit to the customer's account or against cheques and not against cash payment.
- iii) Banks should ensure that the provisions of Foreign Contribution (Regulation) Act, 1976 as amended from time to time, wherever applicable are strictly adhered to.

2.2 KYC Policy

Banks should frame their KYC policies incorporating the following four key elements:

- a) Customer Acceptance Policy;
- b) Customer Identification Procedures;



- c) Monitoring of Transactions; and
- d) Risk Management.

2.3 Customer Acceptance Policy (CAP)

- a) Every bank should develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place on the following aspects of customer relationship in the bank.
 - (i) No account is opened in anonymous or fictitious/benami name(s);
 - (ii) Parameters of risk perception are clearly defined in terms of the nature of business activity , location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorisation of customers into low, medium and high risk (banks may choose any suitable nomenclature viz. level I, level II and level III). Customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs) may, if considered necessary, be categorised even higher;
 - (iii) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and instructions/guidelines issued by Reserve Bank from time to time;
 - iv) Not to open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures i.e. bank is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non cooperation of the customer or non reliability of the data/ information furnished to the bank. It is, however, necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision by a bank to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision;
 - v) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in



conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity and

- vi) Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organisations etc.
- b) Banks should prepare a profile for each new customer based on risk categorisation. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the bank. However, while preparing customer profile banks should take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein should not be divulged for cross selling or any other purposes.
- c) For the purpose of risk categorisation, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorised as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Customers that are likely to pose a higher than average risk to the bank should be categorised as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc. Banks should apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. Examples of customers



requiring higher due diligence include (a) nonresident 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. However, only NPOs/NGOs promoted by United Nations or its agencies may be classified as low risk customer.

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

2.4 Customer Identification Procedure (CIP)

- a) The policy approved by the Board of banks should clearly spell out the Customer Identification Procedure to be carried out at different stages i.e. while establishing a banking relationship; carrying out a financial transaction or when the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data. Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Banks need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship. Being satisfied means that the bank must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based approach is considered necessary to avoid disproportionate cost to banks and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.). For customers that are natural persons, the banks should obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities,



the bank should (i) verify the legal status of the legal person/entity through proper and relevant documents; (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorised 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 paragraph 2.5 below for guidance of banks. Banks may, however, frame their own internal guidelines based on their experience of dealing with such persons/entities, normal bankers' prudence and the legal requirements as per established practices. If the bank decides to accept such accounts in terms of the Customer Acceptance Policy, the bank should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

- b) It has been observed that some close relatives, e.g. wife, son, daughter and daughter and parents etc. who live with their husband, father/mother and son, as the case may be, are finding it difficult to open account in some banks as the utility bills required for address verification are not in their name. It is clarified, that in such cases, banks can obtain an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) wanting to open an account is a relative and is staying with him/her. Banks can use any supplementary evidence such as a letter received through post for further verification of the address. While issuing operational instructions to the branches on the subject, banks should keep in mind the spirit of instructions issued by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.
- c) Banks should introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. The periodicity of such updation should not be less than once in five years in case of low risk category customers and not less than once in two years in case of high and medium risk categories.
- d) An indicative list of the nature and type of documents/information that may be may be relied upon for customer identification is given in



Annex-I to this Master Circular. It is clarified that permanent correct address, as referred to in Annex-I, means the address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other document accepted by the bank for verification of the address of the customer.

- e) It has been brought to our notice that the said indicative list furnished in Annex -I, is being treated by some banks as an exhaustive list as a result of which a section of public is being denied access to banking services. Banks are, therefore, advised to take a review of their extant internal instructions in this regard.

2.5 Customer Identification Requirements - Indicative Guidelines

i) Trust/Nominee or Fiduciary Accounts

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

ii) Accounts of companies and firms

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



iii) 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.

iv) 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 a 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.



v) 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 should 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.

2.6 Small Deposit Accounts

- (i) Although flexibility in the requirements of documents of identity and proof of address has been provided in the above mentioned KYC guidelines, it has been observed that a large number of persons, especially, those belonging to low income group both in urban and rural areas are not able to produce such documents to satisfy the bank about their identity and address. This would lead to their inability to access the banking services and result in their financial exclusion. Accordingly, the KYC procedure also provides for opening accounts for those persons who intend to keep balances not exceeding Rupees Fifty Thousand (Rs. 50,000/-) in all their accounts taken together and the total credit in all the accounts taken together is not expected to exceed Rupees One Lakh (Rs. 1,00,000/-) in a year. In such cases, if a person who wants to open an account and is not able to produce documents mentioned in Annex I of this master circular, banks should open an account for him, subject to:

Introduction from another account holder who has been subjected to full KYC procedure. The introducer's account with the bank should be at least six months old and should show satisfactory transactions.



Photograph of the customer who proposes to open the account and also his address need to be certified by the introducer,

or

any other evidence as to the identity and address of the customer to the satisfaction of the bank.

- ii) While opening accounts as described above, the customer should be made aware that if at any point of time, the balances in all his/her accounts with the bank (taken together) exceeds Rupees Fifty Thousand (Rs. 50,000/-) or total credit in the account exceeds Rupees One Lakh (Rs. 1,00,000/-) in a year, no further transactions will be permitted until the full KYC procedure is completed. In order not to inconvenience the customer, the bank must notify the customer when the balance reaches Rupees Forty Thousand (Rs. 40,000/-) or the total credit in a year reaches Rupees Eighty thousand (Rs. 80,000/-) that appropriate documents for conducting the KYC must be submitted otherwise operations in the account will be stopped.

2.7 Monitoring of Transactions

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



Banks should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers should be carried out at a periodicity of **not less** than once in six months.

2.8 Closure of accounts

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

2.9 Risk Management

- a) The Board of Directors of the bank should ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It should cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility should be explicitly allocated within the bank for ensuring that the bank's policies and procedures are implemented effectively. Banks should, in consultation with their boards, devise procedures for creating risk profiles of their existing and new customers and apply various anti money laundering measures keeping in view the risks involved in a transaction, account or banking/business relationship.
- b) Banks' internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Banks should ensure that their audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Concurrent/ Internal Auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard should be put up before the Audit Committee of the Board on quarterly intervals.



2.10 Introduction of New Technologies - Credit cards/debit cards/ smart cards/gift cards

Banks should pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Many banks are engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Banks are required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Further, marketing of credit cards is generally done through the services of agents. Banks should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that agents are also subjected to KYC measures.

2.11 Combating Financing of Terrorism

- a) In terms of PMLA Rules, suspicious transaction should include inter alia transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. Banks are, therefore, advised to develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit - India (FIU-IND) on priority.
- b) As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank circulates these to all banks and financial institutions. Banks/Financial Institutions should ensure to update the consolidated list of individuals and entities as circulated by Reserve Bank. Further, the updated list of such individuals/entities can be accessed in the United Nations website at <http://www.un.org/sc/committees/1267/consolist.shtml>. Banks are advised that before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the list. Further, banks



should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to RBI and FIU-IND.

- c) Banks are also advised to take into account risks arising from the deficiencies in AML/CFT regime of certain jurisdictions viz. Iran, Uzbekistan, Pakistan, Turkmenistan and Sao Tome and Principe, as identified in FATF Statement of February 25, 2009 circulated to banks vide our circular letter DBOD.AML. No.20716/14.01.027/2008-09 dated June 03, 2009.

2.12 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. Banks should gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Information on the other bank's management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the correspondent's/respondent's country may be of special relevance. Similarly, banks should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. While it is desirable that such relationships should be established only with the approval of the Board, in case the Boards of some banks wish to delegate the power to an administrative authority, they may delegate the power to a committee headed by the Chairman/CEO of the bank while laying down clear parameters for approving such relationships. Proposals approved by the Committee should invariably be put up to the Board at its next meeting for post facto approval. The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented. In the case of payable-through-



accounts, the correspondent bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them. The correspondent bank should also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

b) **Correspondent relationship with a "Shell Bank"**

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.

2.13 Applicability to branches and subsidiaries outside India

The guidelines contained in this master circular shall apply to the branches and majority owned subsidiaries located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of Reserve Bank. In case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of banks are required to adopt the more stringent regulation of the two.

2.14 Wire Transfer

Banks use wire transfers as an expeditious method for transferring funds between bank accounts. Wire transfers include transactions occurring within the national boundaries of a country or from one country to another.



As wire transfers do not involve actual movement of currency, they are considered as a rapid and secure method for transferring value from one location to another.

- i) The salient features of a wire transfer transaction are as under:
 - a) Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. The originator and the beneficiary may be the same person.
 - b) Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institutions are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.
 - c) Domestic wire transfer means any wire transfer where the originator and receiver are located in the same country. It may also include a chain of wire transfers that takes place entirely within the borders of a single country even though the system used to effect the wire transfer may be located in another country.
 - d) The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the bank to perform the wire transfer.
- ii) Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analysing suspicious or unusual activity and disseminating it as necessary. The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold



limits. Accordingly, banks must ensure that all wire transfers are accompanied by the following information:

(A) Cross-border wire transfers

- i) All cross-border wire transfers must be accompanied by accurate and meaningful originator information.
- ii) Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included.
- iii) Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (ii) above.

(B) Domestic wire transfers

- i) Information accompanying all domestic wire transfers of Rs.50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.
- ii) If a bank has reason to believe that a customer is intentionally structuring wire transfer to below Rs. 50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the bank must insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be made to FIU-IND.
- iii) When a credit or debit card is used to effect money transfer, necessary information as (i) above should be included in the message.

(iii) Exemptions

Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions would be exempted from the above requirements.



(iv) Role of Ordering, Intermediary and Beneficiary banks

(a) Ordering Bank

An ordering bank is the one that originates a wire transfer as per the order placed by its customer. The ordering bank must ensure that qualifying wire transfers contain complete originator information. The bank must also verify and preserve the information at least for a period of ten years.

(b) Intermediary bank

For both cross-border and domestic wire transfers, a bank processing an intermediary element of a chain of wire transfers must ensure that all originator information accompanying a wire transfer is retained with the transfer. Where technical limitations prevent full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record must be kept at least for ten years (as required under Prevention of Money Laundering Act, 2002) by the receiving intermediary bank of all the information received from the ordering bank.

(c) Beneficiary bank

A beneficiary bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they should be reported to the Financial Intelligence Unit-India. The beneficiary bank should also take up the matter with the ordering bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information on the remitter, the beneficiary bank should consider restricting or even terminating its business relationship with the ordering bank.

2.15 Principal Officer

- a) Banks should appoint a senior management officer to be designated as Principal Officer. Principal Officer shall be located at the head/corporate office of the bank and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He will maintain close liaison with enforcement agencies,



banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism.

- b) The Principal Officer will be responsible for timely submission of CTR, STR and reporting of counterfeit notes to FIU-IND.

2.16 Maintenance of records of transactions/Information to be preserved/ Maintenance and preservation of records/Cash and Suspicious transactions reporting to Financial Intelligence Unit- India (FIU-IND)

Government of India, Ministry of Finance, Department of Revenue, vide its notification dated July 1, 2005 in the Gazette of India, has notified the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the said Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts certain obligations on the banking companies in regard to preservation and reporting of customer account information. Banks are, therefore, advised to go through the provisions of PMLA, 2002 and the Rules notified there under and take all steps considered necessary to ensure compliance with the requirements of Section 12 of the Act *ibid*.

(i) Maintenance of records of transactions

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

- a) all cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;
- b) 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;
- c) 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 or a document has taken place facilitating the transaction and
- d) all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.



Explanation - Integrally connected cash transactions referred to at (b) above

The following transactions have taken place in a branch during the month of April , 2008:

Date	Mode	Dr. (in Rs.)	Cr. (in Rs.)	Balance (in Rs.) BF-8,00,000.00
02/04/2008	Cash	5,00,000.00	3,00,000.00	6,00,000.00
07/04/2008	Cash	40,000.00	2,00,000.00	7,60,000.00
08/04/2008	Cash	4,70,000.00	1,00,000.00	3,90,000.00
Monthly summation		10,10,000.00	6,00,000.00	

- f) As per above clarification, the debit transactions in the above example are integrally connected cash transactions because total cash debits during the calendar month exceeds Rs. 10 lakhs. However, the bank should report only the debit transaction taken place on 02/04 & 08/04/2008. The debit transaction dated 07/04/2008 should not be separately reported by the bank, which is less than Rs.50,000/-.
- g) All the credit transactions in the above example would not be treated as integrally connected, as the sum total of the credit transactions during the month does not exceed Rs.10 lakh and hence credit transaction dated 02, 07 & 08/04/2008 should not be reported by banks.

(ii) Information to be preserved

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

- the nature of the transactions;
- the amount of the transaction and the currency in which it was denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction



(iii) Maintenance and Preservation of record

- a) Banks are required to maintain the records containing information in respect of transactions referred to in Rule 3 above. Banks should take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. Further, banks should 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.
- b) Banks should ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least ten years after the business relationship is ended. The identification records and transaction data should be made available to the competent authorities upon request.
- c) In paragraph 2.7 of this Master Circular, banks have been advised to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level should be properly recorded. Such records and related documents should be made available to help auditors in their day-to-day work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities. These records are required to be preserved for ten years as is required under PMLA, 2002.



(iv) Reporting to Financial Intelligence Unit - India

- a) In terms of the PMLA rules, banks are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

Director, FIU-IND, Financial Intelligence Unit-India,
6th Floor, Hotel Samrat, Chanakyapuri, New Delhi-110021.
Website - <http://fiuindia.gov.in/>

- b) Banks should carefully go through all the reporting formats. There are altogether eight reporting formats, as detailed in Annex II, viz. i) Cash Transactions Report (CTR); ii) Summary of CTR iii) Electronic File Structure-CTR; iv) Suspicious Transactions Report (STR); v) Electronic File Structure-STR; vi) Counterfeit Currency Report (CCR); vii) Summary of CCR and viii) Electronic File Structure-CCR. The reporting formats contain detailed guidelines on the compilation and manner/procedure of submission of the reports to FIU-IND. It would be necessary for banks to initiate urgent steps to ensure electronic filing of all types of reports to FIU-IND. The related hardware and technical requirement for preparing reports in an electronic format, the related data files and data structures thereof are furnished in the instructions part of the concerned formats.
- c) FIU-IND have placed on their website editable electronic utilities to enable banks to file electronic CTR/STR who are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data base. It is, therefore, advised that in cases of banks, where all the branches are not fully computerized, the Principal Officer of the bank should cull out the transaction details from branches which are not yet computerized and suitably arrange to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND in their website <http://fiuindia.gov.in>.
- d) In terms of instructions contained in paragraph 2.3(b) of this Master Circular, banks are required to prepare a profile for each



customer based on risk categorisation. Further, vide paragraph 2.7, the need for periodical review of risk categorisation has been emphasized. It is, therefore, reiterated that banks, as a part of transaction monitoring mechanism, are required to put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers. It is needless to add that a robust software throwing alerts is essential for effective identification and reporting of suspicious transaction.

2.17 Cash and Suspicious Transaction Reports

a) Cash Transaction Report (CTR)

While detailed instructions for filing all types of reports are given in the instructions part of the related formats, banks should scrupulously adhere to the following:

- i) The Cash Transaction Report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month. Cash transaction reporting by branches to their controlling offices should, therefore, invariably be submitted on monthly basis (**not on fortnightly basis**) and banks should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.
- ii) All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported by the Principal Officer to FIU-IND immediately in the specified format (Counterfeit Currency Report - CCR). These cash transactions should also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.
- iii) While filing CTR, details of individual transactions below Rupees Fifty thousand need not be furnished.
- iv) CTR should contain only the transactions carried out by the bank on behalf of their clients/customers excluding transactions between the internal accounts of the bank.
- v) A summary of cash transaction report for the bank as a whole



should be compiled by the Principal Officer of the bank every month in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted to FIU-IND.

- vi) In case of Cash Transaction Reports (CTR) compiled centrally by banks for the branches having Core Banking Solution (CBS) at their central data centre level, banks may generate centralised Cash Transaction Reports (CTR) in respect of branches under core banking solution at one point for onward transmission to FIU-IND, provided:
 - a) The CTR is generated in the format prescribed by Reserve Bank in Para 2.16(iv)(b) of Master Circular on Know Your Customer (KYC) norms /Anti-Money Laundering (AML) standards/ Combating of Financing of Terrorism (CFT)/ Obligation of banks under PMLA, 2002 dated July 01, 2009;
 - b) A copy of the monthly CTR submitted on its behalf to FIU-IND is available at the concerned branch for production to auditors/inspectors, when asked for; and
 - c) The instruction on 'Maintenance of records of transactions'; 'Information to be preserved' and 'Maintenance and Preservation of records' as contained above in this master circular at Para 2.16 (i), (ii) and (iii) respectively are scrupulously followed by the branch.

However, in respect of branches not under CBS, the monthly CTR should continue to be compiled and forwarded by the branch to the Principal Officer for onward transmission to FIU-IND.

b) Suspicious Transaction Reports (STR)

- i) While determining suspicious transactions, banks should be guided by definition of suspicious transaction contained in PMLA Rules as amended from time to time.
- ii) It is likely that in some cases transactions are abandoned/ aborted by customers on being asked to give some details or to



provide documents. It is clarified that banks should report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

- iii) Banks should make STRs if they have reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.
- iv) 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.
- v) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, banks may consider the indicative list of suspicious activities contained in Annex-E of the IBA's Guidance Note for Banks, 2005.
- vi) Banks should not put any restrictions on operations in the accounts where an STR has been made. Moreover, it should be ensured that there is no tipping off to the customer at any level.

2.18 Customer Education/Employee's Training/Employee's Hiring

a) Customer Education

Implementation of KYC procedures requires banks to demand certain information from customers which may be of personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. There is, therefore, a need for banks to



prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the KYC programme. The front desk staff needs to be specially trained to handle such situations while dealing with customers.

b) Employee's Training

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

c) Hiring of Employees

It may be appreciated that KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking channels. It would, therefore, be necessary that adequate screening mechanism is put in place by banks as an integral part of their recruitment/hiring process of personnel.



Annex- I

Customer Identification Procedure

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

Features	Documents
<p>Accounts of individuals</p> <ul style="list-style-type: none"> - Legal name and any other names used - Correct permanent address 	<ul style="list-style-type: none"> (i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving licence (v) Identity card (subject to the bank's satisfaction) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of bank. (i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority (iv) Electricity bill (v) Ration card (vi) Letter from employer (subject to satisfaction of the bank) (any one document which provides customer information to the satisfaction of the bank will suffice)
<p>Accounts of companies</p> <ul style="list-style-type: none"> - Name of the company - Principal place of business - Mailing address of the company - Telephone/Fax Number 	<ul style="list-style-type: none"> (i) Correct permanent address 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



Features	Documents
	(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 <ul style="list-style-type: none">- Legal name registered- Address- Names of all partners and their addresses- Telephone numbers of the firm and partners	(i) Registration certificate, if (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 <ul style="list-style-type: none">- 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, 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



Annex - II

(List of various reports and their formats)

1. Cash Transaction Report (CTR)
2. Summary of CTR
3. Electronic File Structure - CTR
4. Suspicious Transaction Report (STR)
5. Electronic File Structure - STR
6. Counterfeit Currency Report (CCR)
7. Summary of CCR
8. Electronic File Structure - CCR



Annex - III

**(List of Circulars on 'Know your Customer' and
Monitoring of Cash Transactions)**

Sr. No.	Circular No. and Date	Subject	Gist of instructions
1.	DBOD.BP.BC.92/C.469-76 dated 12th August,1976	Rs.5000/-	Applicants (whether customer or not) for DD/ MT / TT / Travellers cheques for amount exceeding Rs.10,000/- should affix Permanent Income Tax Number on the application.
2.	DBOD.GC.BC.62/c.408(A)/87 dated 11th November, 1987	Frauds in banks- opening of new accounts.	Payment for imports should be made by debit to the accounts maintained with the same bank or any other bank and under no circumstances cash should be accepted for retirement of import bills. There should be reasonable gap of say, 6 months between the time an introducer opens his account and introduces another prospective account holder to the bank. Introduction of an account should enable proper identification of the person opening an account so that the person can be traced if the account is misused.



Sr. No.	Circular No. and Date	Subject	Gist of instructions
3.	DBOD.BP.BC.114/C.469(81)-91 dated 19th April, 1991	Misuse of banking channels for violation of fiscal laws and evasion of taxes - Issue and payment of demand drafts for Rs.50,000 and above.	Banks to issue travellers cheques, demand drafts, mail transfers, telegraphic transfers for Rs.50,000/- and above by debit to customers accounts or against cheques only and not against cash.
4.	DBOD.BC.20/17.04.001/92 dated 25th August, 1992	Committee to enquire into various aspects relating to and frauds malpractices in banks.	Banks advised to adhere to the prescribed norms and safeguards while opening accounts etc.
5.	DBOD.BP.BC.60/21.01.023/92 dated 21st December, 1992	Diversion of working capital funds.	Banks to ensure that withdrawals from cash credit / overdraft accounts are strictly for the purpose for which the credit limits were sanctioned by them. There should be no diversion of working capital finance for acquisition of fixed assets, investments in associate companies / subsidiaries and acquisition of shares, debentures, units of UTI and other mutual funds and other investments in the capital market.



Sr. No.	Circular No. and Date	Subject	Gist of instructions
6.	DBOD.FMC.No.153/ 27.01.003/93-94 dated 1st September, 1993	Monitoring of flow of funds.	Banks to be vigilant and ensure proper end use of bank funds / monitoring flow of funds. Banks to keep vigil over heavy cash withdrawals by account holders which may be disproportionate to their normal trade / business requirements and cases of unusual trends. Doubtful cases to be reported to DBOD, Regional office.
7.	DBOD.GC.BC.193 dated 18th November, 1993	Frauds in banks-	Banks to be vigilant in Encashment of opening new accounts Interest / without proper introduc Dividend tion, new accounts with Warrants, fictitious names and Refund Orders addresses. Banks in etc. structed to strictly adhere to the instructions issued on opening and operating of bank accounts.
8.	DBOD.GC.BC.202/ 17.04.001/93 dated 6th December, 1993	The Committee to enquire into various aspects relating to frauds and malpractices in banks.	Customer identification while opening accounts including obtaining of photographs of customers while opening accounts.



Sr. No.	Circular No. and Date	Subject	Gist of instructions
9.	DBOD.No.GC.BC.46/17.04.001 dated 22nd April, 1994	The Committee to enquire into	Clarifications given to banks regarding obtaining various aspects photographs of the de relating to positors / account holder frauds and authorised to operate new malpractices accounts with effect from in banks. 1.1.1994. Obtaining of photographs would apply to residents and non-residents and all categories of depos its including fixed / recurring / cumulative deposit accounts and also to those persons authorised to oper ate the accounts.
10.	DBOD.BP.BC.106/ 21.01.001/94 dated 23rd September, 1994	Fraudulent operations in deposit accounts -opening and collection of cheques / pay orders etc.	Banks to examine every request for opening joint accounts very carefully, look into the purpose, other relevant aspects relating to business, the financial position of the account holders and whether number of account holders are large. 'Generally crossed' cheques and pay able to' order' should be collected only on proper endorsement by the payee. Banks to exercise care in collection of cheques of large amounts and ensure that joint accounts are not used for benami transactions.



Sr. No.	Circular No. and Date	Subject	Gist of instructions
11.	DBOD.BP.BC.57/21.01.001/95 dated 4th May, 1995	Frauds in banks- Monitoring of deposit accounts.	Banks to introduce system of close watch of new deposit accounts and and monitoring of cash withdrawals and deposits for Rs.10 lakh and above in deposit, cash credit and overdraft accounts. Banks to keep record of details of these large cash transactions in a separate register.
12.	DBOD.BP.BC.102/ 21.01.001/95 dated 20th September, 1995	Monitoring of Deposit Accounts.	Reporting of all cash deposits and withdrawals of Rs.10 lakhs and above with full details in fortnightly statements by bank branches to their controlling offices. Transactions of suspicious nature to be apprised to Head Office. RBI to look into these statements at the time of inspections.
13.	DBOD.BP.BC.42/21.01.001/96 dated 6th April, 1996	Monitoring cash deposits and withdrawals of Rs.10 lakh and above in deposit / other	Banks asked to submit feedback on implementation of the system of close monitoring of large cash deposits and withdrawals of Rs.10 lakh and above accounts.



Sr. No.	Circular No. and Date	Subject	Gist of instructions
14.	DBOD.No.BP.BC.12/21.01.023/98 dated 11th February, 1998	Furnishing of data-violation of secrecy	Banks should satisfy themselves that information sought will not violate obligations. the laws relating to secrecy in banking transactions except under compulsion of law, duty to the public to disclose, where interest of bank requires disclosure and where disclosure is made with the express or implied consent of the customer.
15.	DBS.FGV.BC.56/23.04.001/98-99 dated 21st June, 1999	Report of the Study Group on Large Value Bank Frauds.	Banks advised to implement the main recommendations of the Study Group on Large Value Bank Frauds.
16.	DBOD.COMP.BC.No.130/07.03.23/2000-01 dated 14th June, 2001	Internet Banking in India-Guidelines.	Banking facilities on Internet will be subject to the existing regulatory framework. Banks having physical presence in India only will be allowed to offer banking services over Internet to residents in India and any cross border transactions will be subject to existing exchange control regulations. Banks to establish identity and also make enquiries about integrity and reputation of the prospective customer. Internet accounts should be opened only after proper introduction and physical verification of the identity of the customer.



Sr. No.	Circular No. and Date	Subject	Gist of instructions
17.	DBOD.BP.52/ 21.01.001/2001-02 dated 5th December, 2001	Prevention of Terrorism Ordinance, 2001 -Implementation thereof.	Banks should keep a watchful eye on the transactions of the 23 terrorist organisations listed in the Schedule to the Ordinance. Violations of the extant Acts or normal banking operations must be reported to the appropriate authorities under the Ordinance under advice to RBI. Banks to undertake 'due diligence' in respect of the 'KYC' principle.
18.	DBOD.AML.BC.89/14.01.001/ 2001-02 dated 15th April, 2002	Freezing of funds pursuant to United Nations Security Council Resolution, 1390	Accounts of individuals and entities listed should be immediately frozen as informed by the Security Council Sanctions Committee of the UN. If any transaction is detected involving any of these entities, banks to report to RBI promptly for necessary action.
19.	DBOD.AML.BC.No.102/ 14.01.001/2001-02 dated 10th May, 2002	Monitoring of accounts - compliance with instructions.	Banks should ensure that no new accounts are opened by banned organisations. Banks to strictly adhere to the extant guidelines regarding opening and monitoring of accounts. Banks to confirm having issued instructions for immediate compliance by the branches and controlling offices.



Sr. No.	Circular No. and Date	Subject	Gist of instructions
20.	DBOD.AML.BC.18/14.01.001/2002-03 dated August 16, 2002	Guidelines on "Know Your Customer" norms and "Cash transactions"	First circular on KYC. The customer identification should entail verification through an introductory reference from an existing account holder/a person known to the bank or on the basis of documents provided by the customer. The Board of Directors of the banks should have in place adequate policies that establish procedures to verify the bonafide identification of individual/corporates opening an account. Branches of banks are required to report all cash deposits and withdrawals of Rs.10 lakhs and above as well as transactions of suspicious nature with full details in fortnightly statements to their controlling offices.
21.	DBOD.NO.AML.BC.58/14.01.001/2004-05 dated November 29, 2004	'Know Your Customer' (KYC) Guidelines -Anti Money Laundering Standards	Our guidelines were revisited to make those compliant with FATF recommendations and Basel Committee Report on CDD. Four pronged approach was prescribed to banks based on Customer Acceptance Policy, Customer Identification Procedure, Monitoring of Transaction and Risk Management.



Sr. No.	Circular No. and Date	Subject	Gist of instructions
22.	DBOD.NO.AML.BC.28/ 14.01.001/2005-06 dated August 23, 2005	Know Your Customer Guidelines - Anti-Money Laundering	KYC guidelines on document requirement were relaxed for people belonging to financially disadvantaged sections standards in the society, who could open account with introductory reference.
23.	DBOD.NO.AML.BC.63/ 14.01.001/2005-06 dated February 15, 2006	Prevention of Money Laundering Act, 2002-Obligation of banks in terms of Rules notified thereunder	Reporting mechanism and formats were prescribed to banks to report cash and suspicious transactions to Financial Intelligence Unit- India (FIU-IND).
24.	DBOD.AML.BC.No.77/ 14.01.001/2006-07 April 13, 2007	Wire transfers	Banks were advised to ensure that all wire transfers involving domestic and cross boarder fund transfers are accompanied by full originator information.
25.	DBOD.AML.BC.No.63/ 14.01.001/2007-08 dated February 18, 2008	Know Your Customer (KYC) Norms / Anti Money Laundering (AML) Standards / Combating of Financing of Terrorism (CFT)	Revised guidelines on KYC / AML issued on review of risk categorization of customers; periodical updation of customer identification data and screening mechanism for recruitment / hiring process of personnel.



Sr. No.	Circular No. and Date	Subject	Gist of instructions
26.	DBOD.AML.BC.No.85/14.01.001/2007-08 dated May 22, 2008	Prevention of Money Laundering Act, 2002 - Obligation of banks in terms of Rules notified thereunder.	Revised guidelines issued on CTR and STR by banks to FIU-IND.
27.	DBOD.AML.BC.No.12/14.01.001/2008-09 dated July 1, 2008	Master Circular-KYC norms / AML Standards / CFT / Obligation of Banks under PMLA, 2002	The Master Circular consolidates all the guide lines issued by RBI on KYC / AML / CFT norms up to June 30, 2008