Financial Intelligence Unit - India

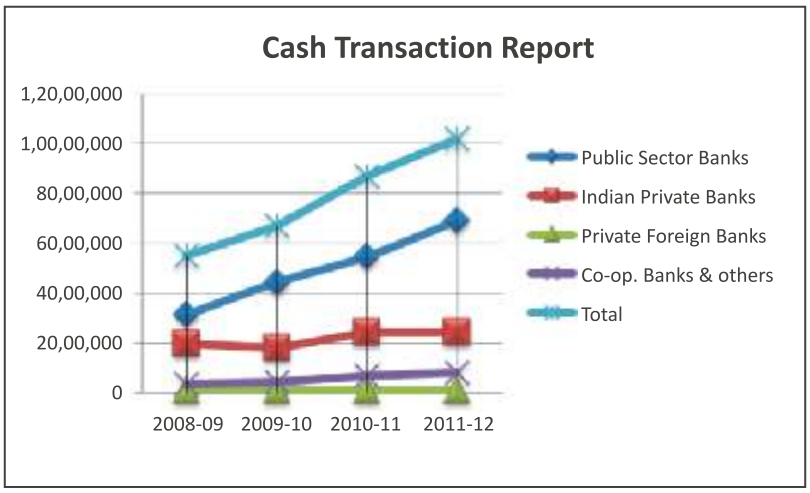
Annual Report 2011-12

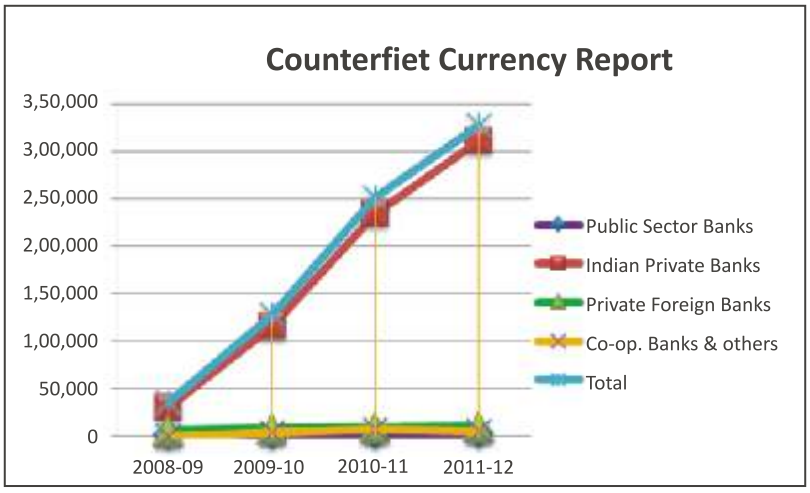
सत्यमेव जयते

Department of Revenue

Ministry of Finance, Government of India

Reports received by FIU-IND over the years





सत्यमेव जयते

Annual Report
2011-12

Department of Revenue
Ministry of Finance, Government of India

सत्यमेव जयते

वित्त मंत्री
भारत
नई दिल्ली – 110001
FINANCE MINISTER
INDIA
NEW DELHI - 110001

January 15, 2013

MESSAGE

I am happy to know that the Financial Intelligence Unit-India (FIU-IND) is publishing its 6th Annual Report. FIU-IND was set up in 2004 in response to international (FATF) standards requiring countries to establish national centres to receive information about money laundering, its predicate offences and terrorist financing. FIU-IND has since been admitted to the Egmont Group of FIUs after a rigorous evaluation. FIU-IND has also put in place robust systems and procedures that meet the major attributes of the international standards-a fact acknowledged and commended in the FATF's follow-up report on India (April,2011).

The FATF standards have undergone substantive changes in 2012, requiring FIUs to put more emphasis on "analysis" of the information received. This has prompted the Egmont Group to start a review of its 1995 charter. I am happy to learn that FIU-IND is a member of the Charter Review Project of the Egmont Group, and also represents the countries of the Asia region in the Egmont Committee.

In order to effectively combat money laundering and terrorism financing, FIU-IND has a challenging task ahead, in enhancing its information processing and analytical capabilities and in equipping itself with personnel and technology to handle the multitude of reporting entities in the financial sectors and the designated non-financial businesses and professions. FIU-IND also has an important role in supporting tax administration and tax collection through exchange of information and collaboration with the tax authorities.

The present Annual Report gives an overview of FIU-IND's operations in 2011-12. I am sure the report will provide the readers useful insight into the operations of FIU-IND.

(P. Chidambaram)

सुमित बोस
सचिव
SUMIT BOSE
SECRETARY

सत्यमेव जयते

भारत सरकार
वित्त मंत्रालय
राजस्व विभाग
नॉर्थ ब्लाक, नई दिल्ली–११०००१
GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF REVENUE
NORTH BLOCK, NEW DELHI-110001
TEL : 011-23092653, 23092111
FAX : 011-23092719
E-mail : rsecy@nic.in
Web : http://finmin.nic.in

MESSAGE

The Financial Intelligence Unit-India (FIU-IND) operates in the legal framework established by the Prevention of Money Laundering Act 2002 (PMLA). FIU-IND performs its basic functions of receipt, analysis and dissemination of information in accordance with the international standards set up by the Financial Action Task Force (FATF) and the Egmont Group of FIUs.

Over the years the information received in FIU-IND has increased exponentially. In 2011-12, FIU-IND received more than 1 crore Cash Transaction Reports, 31,317 Suspicious Transaction Reports and over 3.27 lakh Counterfeit Currency Reports. The collection, storage, analysis and dissemination of this vast amount of information poses major challenges in terms of skills, resources and security. FIU-IND has invested significant resources in upgrading technology to cope with the increasingly higher volume of information and to perform advanced analysis for identity and relationships resolution, a key function to generate actionable intelligence. In the past, FIU-IND has supplied important information and intelligence obtained from domestic and international sources. I am sure the role of FIU-IND in supporting the investigating agencies will continue to increase over time, with maturing of FIU's reporting regime and deepening of international cooperation in information exchange.

The recent passage by Parliament of the amendments to the Prevention of Money Laundering Act, in response primarily to the Financial Action Task Force standards, is intended to equip the FIU-IND with better access to information, and a more structured sanctions regime, in order to improve its effectiveness. The amendments would also enlarge the canvas of reporting entities under the PMLA. These measures would benefit FIU-IND in discharging its responsibilities.

I am happy to note that FIU-IND has also made significant contribution to the Egmont Group of FIUs, where 131 countries are represented. During the year, FIU-IND played a key role in the Egmont initiative to develop an FIU Information System Maturity Model. FIU-IND is also taking active part in the revision of the Egmont Charter. I wish FIU-IND and its staff success in meeting the challenges of fast-changing international environment and fulfilling its national mandate effectively.

(Sumit Bose)

Director's Report

Director's Report

I am happy to present this Annual Report for the year 2011-12. The year was significant for FIU-IND for two reasons. Important changes were proposed in the Prevention of Money Laundering Act (PMLA), which provides the legislative framework for the operation of FIU-IND, to bring the law in harmony with the requirements of the international standards. Alongside, significant progress was made in the development of Project FINnet, a comprehensive online solution for receipt, analysis and dissemination of information by FIU-IND, aimed at putting the FIU at the cutting edge of technology. The project is at the final stage of completion and is expected to be fully operational in the near future.

The year also saw a significant increase in the volume of reports being filed with FIU-IND. The Suspicious Transaction Reports registered an increase of more than 50% over the previous year. The number of reports analyzed and disseminated has also increased two-fold. The number of Cash Transaction Reports increased from 8.68 million in 2010-11 to 10.19 million in 2011-12. The Counterfeit Currency Reports filed by the banks registered a growth of 30%. I am happy to report that FIU-IND was able to cope with the increased volume of work and meet targets in all the key result areas identified despite serious shortage of manpower.

FIU-IND has followed a policy of proactive engagement with the reporting institutions, collaboration with regulators and industry bodies in outreach activities, training of personnel and improving compliance. Recognising the need for a sound system of detecting the suspicious transactions, FIU-IND collaborated with the RBI, IBA and the banking sector to develop red flag indicators for the banking sector. The guidelines for this were issued during the year. FIU-IND carried this initiative forward for the payment system operators and money transfer service providers, with plans to replicate the exercise for the insurance and capital market sectors as well. FIU-IND expects that with the implementation of these guidelines, a robust system for generating STRs will be put in place. In times to come, implementation of these red flag indicators across the reporting entities and their dynamic review to ensure they remain relevant, will remain a key challenge for FIU-IND.

The compliance reviews by FIU-IND have served the purpose of spreading awareness about the importance of AML/CFT and improving the compliance culture among the reporting entities. To boost the compliance function, Reporting Entity Compliance Assessment and Monitoring (RECAM) will be enabled in FINnet for evaluating and managing the compliance lifecycle of an entity.

The recent passage of the amendments to the PML Act brings about significant changes in the legislative framework relevant to the functioning of FIU-IND. Some of these changes relate to:

- Inclusion of additional reporting entities such as entities regulated by Forward Market Commission, members of commodity exchange, India Post, etc. and some of non-financial businesses and professions such as registrar or sub-registrar of properties, real estate agents, dealers in precious metals, precious stones and high value goods, private locker operators, etc.

- Empowering FIU-IND to call for records of transaction or any additional information required by FIU-IND and obligation on the reporting entity to maintain confidentiality of the requested information.

- Broadening the range of sanctions for non-compliance, provision for appointing special auditor for conducting audit in complex cases, and application of sanctions to designated Directors or any employee of the reporting entity.

- Extending 'safe harbour' provision to the reporting entity, its directors and employees against both civil and criminal liabilities for discharging their obligations under PMLA.

These amendments will go a long way in widening and deepening the AML/CFT regime in the country and improving compliance.

Some other significant developments have also taken place with profound implications for FIU-IND. The introduction of KYC Registration Agency (KRA) in the capital market sector, and the efforts to replicate the experience for the entire financial sector have the potential of a paradigm change in the KYC domain with significant economies in the cost of record keeping, ease in performing the KYC process and accessing the KYC information. FIU-IND has been a key stakeholder in the matter and will keep supporting any enterprise to bring about economy, efficiency and effectiveness in the AML/CFT compliance framework.

During the year, FIU-IND contributed significantly to the activities of the Egmont Group. The FIU Information System Maturity Model, in which FIU-IND played a lead role, was approved by the Egmont Group Plenary held at Yerevan, Armenia in July 2011. FIU-IND has taken an active part in the Egmont Group Charter Review Project (CRP), and has contributed to the Legal, Operational and IT working groups of the Egmont Group. FIU-IND has also been re-elected as the Asia region representative in the Egmont Committee of the Egmont Group, giving it an opportunity to participate and contribute to the key policy issues.

Looking to the future, rolling out of the FINnet, which is critically important for improving the operational efficiency of FIU-IND, and implementing the revised legal paradigm of the PMLA will be the two key challenges. The officers and staff of FIU-IND have worked with commendable commitment and professionalism to establish robust systems and procedures, and it will be our endeavour to keep FIU-IND at the forefront of the international fight against money laundering and terrorist financing.

(P K Tiwari)
Director
Financial Intelligence Unit-India

Contents

.

Performance at a Glance: 2011-12

Collection of information

- 10.1 million Cash Transaction Reports (CTRs) received; 99.96% in electronic form
- 31,317 Suspicious Transaction Reports (STRs) received
- 3,27,382 Counterfeit Currency Reports (CCRs) received

Analysis and Dissemination of Information

- 31,279 STRs processed
- 23,688 STRs disseminated

Collaboration with domestic Law Enforcement and Intelligence Agencies

- Regular interaction and exchange of information
- Received 590 requests for information from Intelligence & Law Enforcement agencies
- Provided information in 582 cases requested by the agencies

Regional and global AML/CFT efforts

- 113 requests received from foreign FIUs
- 46 requests sent to foreign FIUs
- 4 MoUs signed with foreign FIUs

Increasing awareness about money laundering and terrorist financing

- Contribution in 76 seminars and training workshops covering 4,031 participants
- Organized the 'Train the Trainer' programme for AML/CFT capacity building with 57 participants.

Improving compliance with the PMLA

- 39 review meetings held with Principal Officers

Strengthening legislative and regulatory framework

- Regular interaction with the Department of Revenue and regulators
- Participation in AML/CFT Regulatory Framework Assessment Committee (ARFAC)

Strengthening IT infrastructure

- FINnet Exchange (FINex) portal was deployed in the production environment
- Registration process for the nodal officers of reporting entities initiated
- Phase II of the Project FINnet provisionally accepted
- Development of performance based reports (KPI, KGI, MIS) completed
- Development of FINcore processes underway

Chapter 1

Financial Intelligence Unit - India

Financial Intelligence Units (FIUs) are specialized government agencies created to act as an interface between financial sector and law enforcement agencies for collecting, analysing and disseminating information, particularly about suspicious financial transactions.

The definition of a FIU has been formalized by the Egmont Group of FIUs follows:

" A central, national agency responsible for receiving, (and as permitted, requesting), analyzing, and disseminating to the competent authorities, disclosures of financial information:

i) concerning suspected proceeds of crime and potential financing of terrorism, or

ii) required by national legislation or regulation in order to combat money laundering and terrorism financing."

Article 7.1.b of the United Nations Convention against Transnational Organized Crime (Palermo Convention) requires member states to consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money laundering.

Recommendation 29 (earlier R26) of the Financial Action Task Force (FATF) also requires countries to establish a FIU to serve as a national centre for receipt and analysis of Suspicious Transaction Reports (STRs) and other information relevant to money laundering, associated predicate offence and terrorist financing, and for the dissemination of the results of that analysis.

Financial Intelligence Unit-India (FIU-IND) is the central national agency for receiving, processing, analyzing and disseminating information relating to suspect financial transactions. FIU-IND was established by the Government of India vide Office Memorandum dated 18th November, 2004 for coordinating and strengthening collection and sharing of financial intelligence through an effective national, regional and global network to combat money laundering and related crimes. It is an independent body reporting to the Economic Intelligence Council (EIC) headed by the Finance Minister. For administrative purposes, FIU-IND is under the Department of Revenue, Ministry of Finance.

FIU-IND is established as an administrative FIU i.e, as an independent government body, that receives, analyses and disseminates STR to the appropriate law enforcement or investigation agency. FIU-IND does not investigate cases.

FIU-IND is headed by the Director, who is of the rank of Joint Secretary to the Government of India. It is an officer-oriented and technology-intensive multi-disciplinary organization and has a sanctioned strength of 75, as per the details given in ***Appendix A***. The chronology of various significant events for FIU-IND is at ***Appendix B***.

As prescribed under the Prevention of Money Laundering Act (PMLA) and the rules framed thereunder, FIU-IND receives reports on cash transactions, suspicious transactions, counterfeit currency transactions and funds received by non profit organisations. These reports are filed by the reporting entities i.e. banks, financial institutions and capital market intermediaries. FIU-IND analyzes the reports received and shares intelligence with agencies specified in Section 66 of PMLA or notified thereunder.

Reports filed under PMLA

- Cash Transaction Reports (CTR)
- Suspicious Transaction Reports (STR)
- Counterfeit Currency Report (CCR)
- NPO Report (NTR)

FIU-IND maintains a national database of financial transactions reported to it and shares this information with enforcement and intelligence agencies on request.

FIU-IND also monitors and identifies strategic and key money laundering trends, typologies and developments based on the analysis of its database.

Vision, Mission and Strategic Goals of FIU-IND

FIU-IND has defined its vision, mission statement and strategic objectives in order to provide a framework for an enterprise wide performance management and to enhance its effectiveness.

Organization Vision

To become a highly agile and trusted organization that is globally recognized as an efficient and effective Financial Intelligence Unit

Mission Statement

To provide quality financial intelligence for safeguarding the financial system from the abuses of money laundering, terrorism financing and other economic offences

FIU-IND, in order to achieve its mission of providing quality financial intelligence for safeguarding the financial system from the abuse of money laundering, terrorist financing and other economic offences, has set three strategic objectives as under:

- Combating Money Laundering, Financing of Terrorism and other economic offences
- Deterring Money laundering and Financing of Terrorism
- Building and strengthening organizational capacity

These objectives are proposed to be achieved through the following thrust areas:

- Effective collection, analysis and dissemination of information
- Enhanced domestic and international cooperation
- Building capacity of reporting entities
- Ensuring compliance with reporting obligations under PMLA
- Building organizational resources
- Strengthening IT infrastructure.

This Report analyses the performance of FIU-IND during the year 2011-12 under the above mentioned thrust areas.

Action Plan for 2011-12

The Action Plan lists out the main objectives of the organization, actions proposed to achieve these objectives and the progress made in implementing these actions. Overall the key result areas (KRAs) showed better performance over the previous year, as shown in the last column of the Table- 1.

Table 1:Action Plan for the year 2011-12

Sl. No.	Major Objective	Actions required to achieve the objective	Success indicators for monitoring/ achieving the objective	Targets for 2011-12	Result
1	Receiving reports in electronic format	i) Assisting reporting entities by providing enabling tools ii) Enhanced outreach programmes	Majority of reports are received in electronic format	More than 99.8% reports in electronic format	Percentage of reports received was 99.96 %
2	Timely processing, analysis and dissemination of Suspicious Transaction Reports (STRs)	Regular processing of STRs	Number of STRs processed and analyzed	STRs pending for processing should not exceed the no. of STRs received in a month	Target Achieved; 31,279 STRs were processed out of 33,092 STRs. During March 2012, 5171 STRs were received
3	Improving quality of analysis	i) Access to LEA/IA databases ii) Increase in analytical staff iii) Detailed analysis of category 'A' STRs	Better quality of dissemination notes	Better quality of analysis with value addition in category 'A' STRs	During the year 532 category 'A' STRs, were disseminated to LEAs/IAs
4	Improving compliance with reporting obligations under PMLA by the reporting entities	i) Monitoring implementation of AML software by the reporting entities ii) Regular review meetings with reporting entities	Submission of STRs by new entities	- At least 20 review meetings with reporting entities - Receipt of STRs from at least 20 new entities	-39 review meetings with reporting entities were held. - Receipt of STRs were reported from 66 new entities.
5	Stabilising reporting regime in respect of authorized persons, casinos and payment system operators	i) Finalisation of reporting formats ii) Outreach activities for new reporting entities	Commencement of reports from new reporting entities	Stabilization of reporting from authorized persons, casinos and payment system operators	During the year 12,655 STRs were filed by this category of reporting entities.
6	Improving information exchange with domestic IAs/LEAs	i) Periodic meetings with domestic IAs/LEAs ii) Training to LEA/IA staff	Increase in information exchange with IAs/LEAs	At least 200 exchanges with domestic agencies	590 requests received from domestic agencies; Replies sent in 582 cases.
7	Enhanced international cooperation	i) Substantial increase in exchange of information with foreign FIUs ii) Negotiation of MOUs with more FIUs	Number of cases in which information is exchanged	At least 125 exchanges with foreign FIUs	More than 159 exchanges with foreign FIUs
8	Project FINnet	i) Implementation of online gateway to receive reports ii) Implementation of analysis and dissemination system	Online receipt of reports from reporting entities	Operationalisation of online gateway.	FINgate portal application was deployed in production environment after security assessment.

Chapter 2

Legal framework

Prevention of Money Laundering Act, 2002

The Prevention of Money Laundering Act, 2002 (PMLA) is India's legislation for combating money laundering. The objective of this act is to prevent money laundering and to provide for confiscation of property derived from or involved in money laundering. The Unlawful Activities (Prevention) Act, 1967 (UAPA) is the legislation to combat terrorism and its financing.

Section 3 of PMLA criminalizes the activity of money laundering as follows:

> *"Whoever, 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" is the property derived directly or indirectly as a result of criminal activity relating to an offence included in the Schedule to PMLA.

Section 4 of PMLA lays down the punishment for the offence of money laundering. A person who commits the offence of money laundering is liable for punishment of rigorous imprisonment for a term of not less than three years, extending upto seven years as well as a fine up to five lakh rupees. The punishment may extend up to ten years if the predicate offence involves drug trafficking. The property derived from or involved in money laundering is also liable for confiscation under PMLA.

The predicate offences for PMLA are included in the Schedule to the Act. There are 3 parts of the schedule; Part A

incorporates crimes against the state, terrorism, drug related crimes, and other serious crimes; Part B incorporates crimes against property & individuals, economic crimes, etc.*;* and Part C includes cross-border crimes. There is a monetary threshold of Rs.30 lakh (Rs.3 million) for Part B of the Schedule. There are no thresholds for Parts A & C. The Schedule includes 156 offences under 28 different laws. A list of predicate offences is at ***Appendix C***.

PMLA incorporates two different sets of provisions; one relating to maintenance and submission of information to FIU and the second relating to investigations into cases of money laundering and powers of search, seizure, collection of evidence, prosecution, etc.

The Director, FIU-IND is the relevant authority for the purpose of the provisions relating to maintenance of records and filing of information. The Directorate of Enforcement is the authority for the provisions relating to search, seizure, confiscation of property, prosecution, etc.

A list of important Rules under PMLA is given at ***Appendix D***. A List of important circulars/ instructions on AML/CFT issued by financial sector Regulators is at ***Appendix E***

Proposed Amendments to PML Act

With a view to make the PML Act more effective and to align it further to the international standards, a number of amendments to the Act have been proposed by the Government through the introduction of Prevention of Money Laundering (Amendment) Bill, 2011. The Bill has been examined by the Parliament's Standing Committee on Finance and their recommendations have been considered by the Government. The revised Bill is expected to be considered by the Parliament during the Winter Session (Nov-Dec, 2012). The following are the

Overview of PMLA

Chapter	Section	Title
I	1-2	Preliminary
II	3-4	Offence of Money Laundering
III	5-11	Attachment, Adjudication and confiscation
IV	12-15	Obligation of the Banks, Financial Institutions and Intermediaries.
V	16-24	Summons, Searches and Seizures, etc.
VI	25-42	Appellate Tribunal
VII	43-47	Special Courts
VIII	48-54	Authorities
IX	55-61	Reciprocal arrangements for assistance in certain matters and procedure for confiscation of property.
X	62-75	Miscellaneous
Schedule	Part A	Offences which are covered regardless of the value
	Part B	Offences which are covered if the value exceeds Rs. 30 Lakhs or more
	Part C	Offence of cross border implications

important amendments relevant to the working of FIU-IND proposed under the Amendment Bill:

A. Inclusion of additional financial sector entities under PMLA:

Amendments are proposed to include following financial sector entities under PMLA:

a) Entities regulated by the Forward Market Commission (Commodity Exchanges)

b) Members of Commodity Exchanges (Commodity Brokers)

c) Entities regulated by the Pension Fund Regulatory Authority (Pension funds)

d) Recognized stock exchanges under Securities Contracts (Regulation) Act

e) India Post, which provides a number of public financial services

B. Inclusion of additional non-financial business and professions under PMLA

The proposed amendment introduces a new category viz, "person carrying on designated business or profession" under Section 2(1)(sa) to cover the following :

- Registrar or Sub-Registrar appointed under section 6 of the Registration Act, 1908 (16 of 1908),
- Real estate agent, as may be notified by the Central Government,
- Dealer in precious metals, precious stones and other high value goods and,
- Person engaged in safekeeping and administration of cash and liquid securities on behalf of other persons.

The obligations under PMLA shall apply to the above persons only when notified by the Central Government.

C. Access to information

Amendment has been proposed to explicitly mention the powers of the Director FIU-IND to call for records of transactions or any additional information that may be required. A separate sub-section has been included to put an obligation on the reporting entity to maintain confidentiality of the request.

D. Sanctions for non-compliance

To strengthen the ability of FIU-IND to ensure compliance, following amendments are proposed:

- Provision for appointment of special auditor for conducting audit in complex cases.
- Provision for sanctions to apply to the designated director or any employee of the reporting entity for non-compliance.
- Expanding the range of sanctions to include warning in writing; directions to comply with specific instructions; and direction to send reports on the measures it is taking.

E. Protection from civil or criminal proceedings

Necessary amendments have been proposed to give protection to Directors as well as employees of a reporting entity from criminal and civil liability for breach of any restriction on disclosure of information.

F. Authorities required to assist in the enforcement of the Act

The list of officers designated under section 54 to assist the authorities in the enforcement of this Act is proposed to be broadened to include officers of the following Departments/ organizations:

- Insurance Regulatory and Development Authority
- Department of Posts
- Forward Markets Commission
- Pension Fund Regulatory and Development Authority

- Registrar or Sub-Registrar appointed under section 6 of the Registration Act, 1908 (16 of 1908);
- Registering authority empowered to register motor vehicles under Chapter IV of the Motor Vehicles Act, 1988 (59 of 1988)
- Recognised stock exchange referred to in clause (f) of section 2 of the Securities Contracts (Regulation) Act, 1956 (42 of 1956);
- The Institute of Chartered Accountants of India (ICAI)
- The Institute of Cost and Works Accountants of India (ICWAI)
- The Institute of Company Secretaries of India (ICSI)

The Unlawful Activities (Prevention) Act, 1967

The legislative measures for combating financing of terrorism in India are contained in the Unlawful Activities (Prevention) Act, 1967 (UAPA). UAPA criminalizes terrorist acts and raising of funds for terrorist acts. The punishment for such an offence is death or imprisonment for life, if the terrorist act results in death of a person. In other cases, the punishment is imprisonment for not less than 5 years but may extend to imprisonment for life. UAPA also makes the act of raising funds for a terrorist organization an offence liable for punishment with imprisonment upto 14 years. The scope of terrorist financing under UAPA includes the act of raising or collecting funds or providing funds to any person or attempting to provide funds to a person to commit / attempt to commit a terrorist act. UAPA also enables forfeiture of proceeds of terrorism including proceeds held by a terrorist organisation or by a terrorist gang. The Act also gives effect to UNSCR 1267 and 1373, enabling freezing, seizing or attaching funds and other financial assets held by designated individuals or entities. Offences under UAPA are included as predicate offences under PMLA in Part A of the Schedule, without any monetary thresholds.

Section 17 of UAPA reads as under:

"Whoever, in India or in a foreign country, directly or indirectly, raises or collects funds or provides funds to any person or persons or attempts to provide funds to any person or persons, knowing that such funds are likely to be used by such person or persons to commit a terrorist act, notwithstanding whether such funds were actually used or not for commission of such act, shall be punishable with imprisonment for a term which shall not be less than five years but which may extend to imprisonment for life, and shall also be liable to fine".

The above provision makes it clear that it is not relevant whether the funds were actually used for the commission of terrorist acts or not, nor is it necessary that the offence of raising or providing or collection of funds be linked to a particular terrorist act. The term "terrorist act" is defined in Section 15 of UAPA.

Section 40 of UAPA criminalizes raising of funds for terrorist organizations listed in the Schedule to UAPA and reads as under:

"A person commits the offence of raising fund for a terrorist organisation, who, with intention to further the activity of a terrorist organisation, (a) invites another person to provide money or other property, and intends that it should be used, or has reasonable cause to suspect that it might be used, for the purposes of terrorism; or (b) receives money or other property, and intends that it should be used, or has reasonable cause to suspect that it might be used, for the purposes of terrorism; or (c) provides money or other property, and knows, or has reasonable cause to suspect, that it would or might be used for the purposes of terrorism. A person, who commits the offence of raising fund for a terrorist organisation under sub-section (1), shall be punishable with imprisonment for a term not exceeding fourteen years, or with fine, or with both".

Section 51 of UAPA allows the Government to freeze, seize or attach funds held by the individuals or entities engaged in terrorism. 35 entities including entities covered under UNSCR 1267 have been declared as terrorist organizations by MHA under UAPA, 1967.

PMLA and FIU-IND

Sections 12 of PMLA requires every banking company, financial institution and intermediary (referred to as reporting entities) to furnish information of prescribed transactions to the Director, FIU-IND and to verify the identity of all its clients in the manner prescribed. The reporting entities are also required to maintain and preserve records of transactions and records of identity of clients for a period of ten years from the date of cessation of transactions.

The relevant Rules prescribe the requirements for maintenance of records and reports to be submitted to FIU-IND. The reporting obligations of financial sector entities are summarized at ***Appendix F***.

Section 13 of PMLA empowers Director, FIU-IND to call for records maintained by a reporting entity and to enquire into cases of suspected failure of compliance with the provisions of PMLA. The Director, FIU-IND is also empowered to impose under Section 13 fine for non-compliance which shall not be less than ten thousand rupees and may extend to one lakh rupees for each failure to comply with PMLA.

Section 69 of PMLA enables the recovery of fines imposed by the Director if they are not paid within six months from the date of imposition of fine and the powers of a Tax Recovery Officer under the Income-tax Act, 1961 can be exercised for this purpose. The fines so imposed are recovered in the same manner as prescribed in Schedule II of the Income-tax Act, 1961 for the recovery of arrears.

Reporting Entities (including those proposed in the PMLA amendment, shown in italics)

Banking Companies
- Public Sector Banks
- Private Indian Banks
- Private Foreign Banks
- Co-operative Banks
- Regional Rural Banks

Financial Institutions
- Insurance Companies
- Hire purchase Companies
- Chit fund Companies
- Housing Finance Institutions
- Non-banking Financial Companies
- Payment System Operators
- Authorized Money Changers
- *India Post*

Intermediaries
- Stock brokers; Sub-brokers
- Share transfer agents
- Registrars to issue
- Merchant bankers
- Underwriters
- Portfolio managers
- Investment advisers
- Depositories and DPs
- Custodian of securities
- Foreign institutional investors
- Venture capital funds
- Mutual funds
- *Intermediary regulated by FMC*
- *Intermediary regulated by PFRDA*
- *Recognized stock exchanges*

DNFBP
- Casino
- *Registrar of Sub-registrar*
- *Real Estate Agent*
- *Dealer in precious metals, precious stones and other high value goods*
- *Private Locker Operators (upon notification)*

Chapter 3

Collection, Analysis and Dissemination of Information

The foundation of FIU-IND's work is collection of prescribed reports that can be analysed and disseminated to partner agencies for use in investigation. The financial data collected from the reporting entities has proven to be of considerable value in money laundering, terrorist financing and other crimes investigated by law enforcement agencies.

FIU-IND's Project FINnet would greatly enhance the efficiency and effectiveness of FIU-IND's core function viz., collection, analysis and dissemination of financial information through IT enablement of key processes.

The number of STRs received, analyzed and disseminated has shown increasing trend. Focussed attention on thrust areas ensured that quality of reporting was maintained and reports received were analyzed and disseminated in time.

Collect information

Section 12 of the PMLA and rules framed thereunder require all reporting entities to furnish to FIU-IND, information relating to prescribed cash transactions, suspicious transactions, transactions of forged or counterfeit currency notes and transactions in accounts of non-profit organizations. As part of the IT modernization programme, FIU-IND has reviewed the existing formats of all the reports required to be submitted and has converged the reporting formats into three; accounts based reporting format; transactions based reporting format; and reporting format for CCRs. These new formats would be used for uploading reports on the FINnet portal.

Cash Transaction Reports

PMLA requires banks, financial institutions and capital market intermediaries to furnish to FIU-IND, information relating to-

- All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency, and
- All series of cash transactions integrally connected to each other, which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month.

Trends in CTRs

- 10.19 million CTRs were reported in 2011-12 as compared to 8.68 million CTRs in the previous year.
- CTRs from the smaller banks such as cooperative banks and regional rural banks increased from 0.67 million in 2010-11 to 0.80 million in 2011-12 mainly due to technical assistance, training and focussed outreach programs undertaken by FIU-IND.
- Reporting from Public Sector Banks continued to show a rising trend from 5.46 million CTRs in 2010-11 to 6.9 million in 2011-12.

Cash Transaction Reports are to be reported on a monthly basis by the 15th day of the month following the month of transaction.

Continuing with the trend, majority of the CTRs received during the year were from Public Sector Banks. The reporting of CTRs from the smaller banks has also increased. FIU-IND continued its effort to ensure that the smaller banks such as district co-operative banks and regional rural banks submit CTRs in electronic format. The quality of reports received is continuously monitored and feedback is provided to individual reporting entities for improving data quality. During the year, around 10.19 million CTRs were received, registering an increase of 17.4 % from the previous year.

Table 2

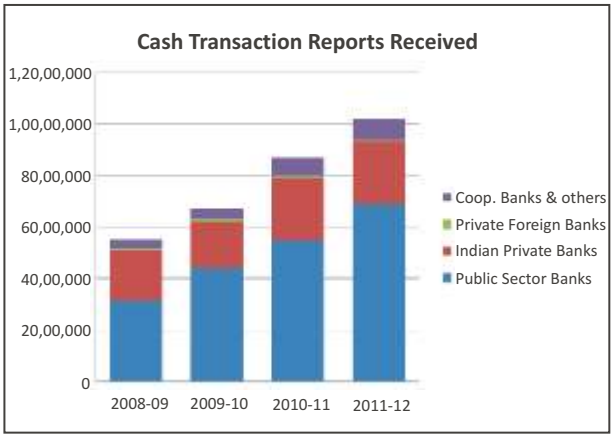


Table 2: Receipt of Cash Transaction Reports from Banking Companies

Type of Bank	2008-09	2009-10	2010-11	2011-12	Till 31st March 2012
Public Sector Banks	31,08,675	44,13,849	54,63,252	69,03,096	**2,28,73,211**
Indian Private Banks	19,80,045	17,84,665	24,42,286	24,06,855	**1,14,01,738**
Private Foreign Banks	88,239	84,428	1,05,288	83,665	**5,06,531**
Co-operative Banks and others	3,34,191	4,11,462	6,76,281	8,04,646	**24,10,124**
Total	**55,11,150**	**66,94,404**	**86,87,107**	**1,01,98,262**	**3,71,91,604**
% of Electronic Reports	99.80%	99.94%	99.94%	99.96%	99.68%

This table shows the number of Cash Transaction Reports (CTRs) submitted by various categories of banks. A CTR covers details of account, related persons and transactions for a month in a bank account.
'Cooperative Banks and others' include urban co-operative banks, district co-operative banks, state co-operative banks and regional rural banks and other entities such as NBFCs and insurance companies.

Suspicious Transaction Reports

Under PMLA, reporting entities are required to report suspicious transactions to FIU-IND. Rule 2(1)(g) of the PMLA Rules defines a suspicious transaction as a transaction, whether or not made in cash, which to a person acting in good faith -

(a) gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime of an offence specified in the Schedule to the Act, regardless of the value involved; or

(b) appears to be made in circumstances of unusual or unjustified complexity; or

(c) appears to have no economic rationale or bonafide purpose; or

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

[Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism]

Majority of the STRs submitted by the reporting entities fall in the sub-clause (b) and (c) of the definition of suspicious transaction.

Trends in STRs *(Table 3)*

- There was more than 50% growth in STRs received in 2011-12 as compared to 2010-11.
- STRs received from Financial Institutions showed maximum growth of 110% in 2011-12 compared to 2010-11 followed by Banks (21.66 %) and Intermediaries (17.86%) .
- Amongst Financial Institutions, Money Transfer Service Agents filed maximum STRs.

Suspicious Transaction Reports (STRs) are required to be reported by the principal officer within 7 working days on being satisfied that the transaction is suspicious.

The "Train the Trainers" programme conducted once a year by FIU-IND has produced the desired cascading effect in spreading AML/CFT awareness across the reporting entities. Data collected from the banks showed that the resource persons who were trained, in turn imparted training to a large number of employees in their respective organization. The AML/CFT programs of the larger entities were closely monitored through regular interactions with their AML teams during which the shortcomings of their report were discussed. Feedback on the quality of STRs reported and suggestions for improvement of quality of STRs were also provided.

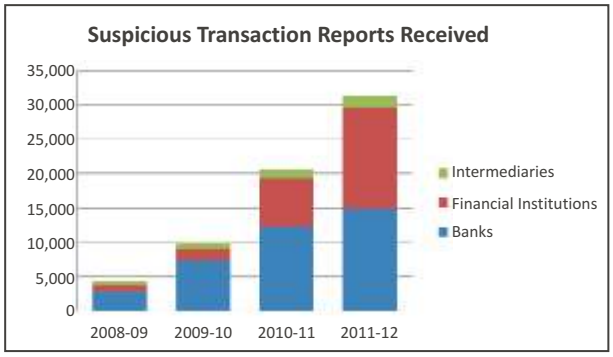


Table 3- Receipt of Suspicious Transaction Reports

Category	2008 - 09	2009-10	2010-11	2011-12	Total till 31.3.12
Banks	2826	7,394	12,287	14,949	**39,076**
Financial Institutions	841	1,655	7,006	14,712	**24,590**
Intermediaries	742	1,018	1,405	1,656	**5,558**
Total	**4409**	**10,067**	**20,698**	**31,317**	**69,224**

This table shows the number of Suspicious Transaction Reports (STRs) submitted by various categories of reporting entities. An STR includes details of all accounts, transactions, individuals and legal persons/entities related to a suspicious transaction.

Identification of Red Flag Indicators(RFIs) for detection of suspicious transactions

In 2011, FIU-IND was actively involved in a Working Group formed by the Indian Banks' Association (IBA) with representatives from selected banks and Reserve Bank of India to review the alert generation scenarios and identify measures to increase the effectiveness of the STR reporting regime. The purpose of the report prepared by the working group is to:

- Create a common and shared understanding among the banking sector, regulators and FIU about the implementation of STR detection and reporting systems
- Provide indicative lists of high risk customers, products, services and geographies
- Provide a list of commonly used alert indicators for detection of suspicious transactions
- Provide guidance for an effective alert management and preparation of STRs

In terms of the business risk categories, the document draws on the FATF's Risk-based Approach Guidance Document; and, in terms of the alert indicators, it differentiates between those that are relevant at the branch level and those that apply at the level of the centralised AML monitoring unit. The report identified 88 red flag indicators relating to 10 sources of alert: (refer to figure below)

Banks will have to select the appropriate number and value thresholds before implementing the alert indicators. Banks are also encouraged to implement additional alert indicators to address specific risks faced by them. The report of the working group has been circulated by the Indian Banks' Association (IBA) to the member banks in May 2011.

Figure: Sources of alerts for banking sector

Source of Alert	Explanation	Number of indicators
Customer Verification	Detected during customer acceptance, identification or verification (excluding reasons mentioned in other codes) (e.g. Use of forged ID, wrong address etc.)	6
Law Enforcement Agency Query	Query or letter received from law enforcement agency (LEA) or intelligence agency (e.g. blocking order received, transaction details sought etc.)	2
Media Reports	Adverse media reports about customer (e.g. newspaper reports)	2
Employee Initiated	Employee raised alert (e.g. behavioral indicators such as customer had no information about transaction, attempted transaction etc.)	14
Public Complaint	Complaint received from public (e.g. abuse of account for committing fraud etc.)	1
Business Associates	Information received from other institutions, subsidiaries or business associates (e.g. cross-border referral, alert raised by agent etc.)	2
Watch List	The customer details matched with watch lists (e.g. UN list, Interpol list etc.)	4
Transaction Monitoring	Transaction monitoring alert (e.g. unusually large transaction, increase in transaction volume etc.)	17
Typology	Common typologies of money laundering, financing of terrorism or other crimes (e.g. structuring of cash deposits etc.)	26
Risk Management System	Risk management system based alert (e.g. high risk customer, country, location, source of funds, transaction type etc.)	14
	Total	88

Note : Indicators are circumstances that indicate suspicious nature of transactions. Suspicious transaction may be detected from one indicator or a set of indicators.

Counterfeit Currency Reports

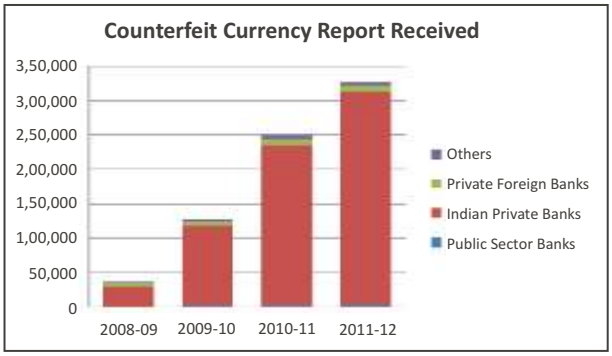
PMLA and Rules thereunder require banking companies to report all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions.' The new format for reporting of Counterfeit Currency Reports (CCRs) have been issued along with utility for generation.

Trends in CCRs

- Around 30% growth in CCRs received during 2011-12 as compared to 2010-11
- 3,27,382 CCRs received in 2011-12 as compared to 2,51,448 CCRs in 2010-11 and 1,27,781 CCRs in 2009-10.
- As of March 2012, FIU-IND has received information about 7,50,921 incidents of detection of Fake Indian Currency Notes (FICN) with a face value of over Rs.60 Crore

During the year, CCR reporting continued to remain a thrust area.

The private Indian Banks contributed majority of CCRs. ***(Table 4)*** The compliance of the public sector banks continued to be low. The matter was taken up with the RBI to take steps to improve compliance by the public sector banks, the best practices of private Indian banks in detection of FICN and reporting to FIU-IND were highlighted.



Process information

Timely processing of information is key to the success of an FIU. For FIU-IND, it has continued to be a focus area. The information received from reporting entities was analyzed and linked, and intelligence reports were disseminated to the partner agencies.

Table 4 - Counterfeit Currency Reports received

Reporting Entity Type	2008-09	2009-10	2010-11	2011-12	Total
Public Sector Banks	396	1,391	1,896	2,649	6,413
Indian Private Banks Private	29,846	1,15,720	2,34,400	3,10,714	6,98,068
Foreign Banks	5,422	7,099	7,936	9,273	30,841
Others	66	3,571	7,216	4,746	15,599
Total	**35,730**	**1,27,781**	**2,51,448**	**3,27,382**	**7,50,921**

This table shows the number of Counterfeit Currency Reports (CCRs) submitted by various categories of banks. A CCR includes details of an instance of counterfeit currency detected by a bank.

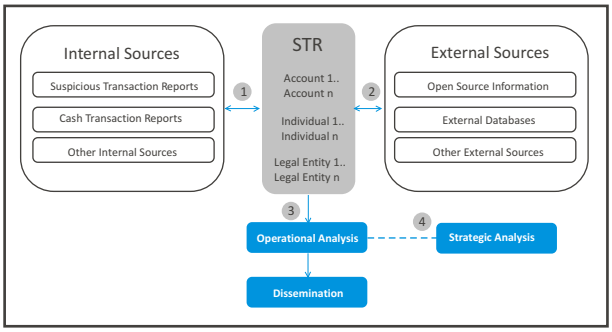
Analysis of STRs

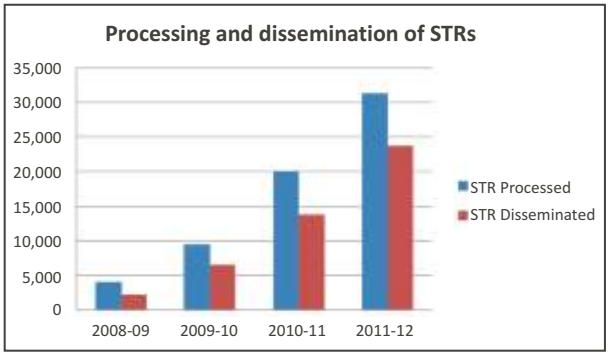
The revised standards (Recommendation 29) issued by FATF in February 2012, require that an FIU should be able to receive and analyze suspicious transaction reports and other information relevant to money laundering, associated predicate offence and terrorist financing and to disseminate the result of that analysis. The interpretive notes to recommendation 29 further clarify that based on the FIU's analysis, the dissemination of information should be selective and allow the recipient authorities to focus on relevant cases/information. The revised standard has laid stress on the performance of analysis function by an FIU.

FIU-IND has built strategies to enhance the analysis process and make the end product more meaningful for the partner agencies. Standard methodologies were developed and adopted for achieving better results in linking and analysis of information. Internal and external data sources were used effectively with the use of technology. Any analysis and linking process must result in actionable intelligence reports and this remained the underlying principle in the methodologies and processes adopted. Emphasis was placed on receiving feedback from the partner agencies and such feedback was used to review and continuously improve the analysis process

as well as the quality of reports received from the reporting entities.

Facts reported in the STR were linked with other internal/external information and interpreted with a view to identify underlying information relevant to a partner agency. Appropriate use of technology for searching and linking the additional information (such as





related addresses, individuals, entities and accounts) in respect of subjects of STRs was made through an in-house search engine. The new capabilities built in FINcore (analysis module of Project FINnet) for effective identity and relationship resolution and linking of records is going to give a boost to the analysis function in the coming years.

While analysing an STR, inter alia, the following factors are considered for deciding whether the STR should be disseminated and to which agency:

- type of suspicion reported in STR
- nature of suspected offence
- value and pattern of transaction in the STR
- linkage with other reports/information maintained with FIU-IND (CTR, etc)
- value and pattern of transaction in linked reports
- linkage with earlier related reference received from domestic agencies or foreign FIUs
- linkage with information available in public domain or additional information with law enforcement agencies

Analysis of CTR database

FIU-IND has developed, an in-house search engine that can compare a search string with the information in FIU's databases and can generate search results ranked on the basis of degree of match. The search results are arranged in a descending order such that the most relevant results are displayed at the top. This enhances the quality of searching and linking process adopted by the analysts at FIU-IND and adds value to the suspicious transaction reports received. This search engine also enables FIU-IND to provide timely response to law enforcement and intelligence agencies on information requested by them.

The CTR database is also subjected to bulk search using unique identifiers such as PAN, which produces faster and more accurate matches. The internal linking process developed in-house enables FIU-IND to create multiple unified views for each account, individual, legal person and address reported in different CTRs. This enables the

Table 5 : Analysis of Suspicious Transaction Reports

Category	2008-09	2009-10	2010-11	2011-12	Total till 31.3.2012
STRs received	4,409	10,067	20,698	31,317	**69,224**
STRs brought forward from previous year	86	476	1,118	1,775	--
STRs Processed	4,019	9,425	20,041	31,279	**67,411**
STRs Disseminated	2,270	6,571	13,744	23,689	**47,600**

The CTR database is used for :

- Processing of STR
- Processing of request for information from
- LEAs/IAs
- Foreign FIU
- CTR Analysis Reports
- Cluster of CTRs related to
  - High Risk Businesses
  - High Risk Geographic Locations
- Threshold Analysis (High Value Transaction)
- Recovery of uncollectible tax demand
- Matching of AIR information with CTR database to find out incidence of cash transaction near the date of property purchase and sale
- Identification of non-filers and stop filers of Income tax

FIU-IND analysts to access in a unified view all relevant details such as IDs, related addresses, related persons and related accounts. The unified view has also been integrated with the search string facility to make FIU-IND database searches more meaningful and effective. This ensures that all related information available about a subject can be viewed on a single page. This also reduces time for multiple searches and has substantially improved ability to disseminate meaningful intelligence as all relevant information is extracted in a single view.

FIU-IND's CTR database is used for the analysis of STRs and for processing requests for information from law enforcement and intelligence agencies. In addition, FIU-IND also carries out analysis of the CTR database on the request of individual agencies. As in the earlier years, the CTR data was also processed on the basis of multiple logical criteria and intelligence reports were generated using data mining and clustering.

Dissemination

FIU-IND disseminates STRs which are considered relevant for investigation by law enforcement/ intelligence agencies based on the nature of suspicion, predicate offence involved and other relevant information linked with the STR. Meetings of analyst groups are conducted to discuss analyzed reports and decide which cases should be disseminated to which law enforcement / intelligence agencies.

Dissemination of actionable and relevant financial intelligence enables FIU-IND to strengthen the work of partner law enforcement and intelligence agencies. Some of the STRs were also disseminated to financial sector regulators and foreign FIUs. Statistical information relating to dissemination of intelligence reports during the year 2011-12 is in ***Table 6.*** Some STRs are disseminated to more than one agency and hence, the

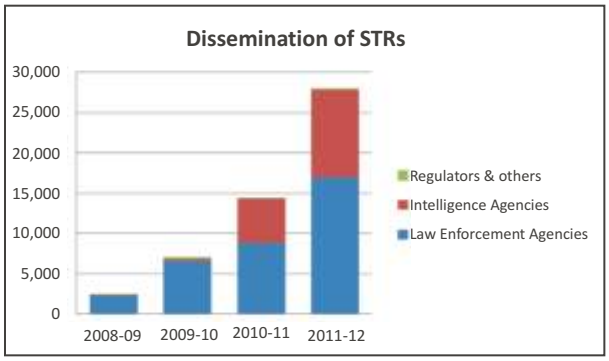


Table 6 - Dissemination of STRs

Type of Agency	2008-09	2009-10	2010-11	2011-12	Total till 31.3.2012
Law Enforcement Agencies	2,319	6,537	8,818	16,905	35,810
Intelligence Agencies	90	362	5,523	10,905	16,989
Regulators & others	41	128	127	225	585
Total	**2,450**	**7,027**	**14,468**	**28,035**	**53,384**

This table shows the number of disseminations to various agencies. Law Enforcement Agencies have the highest share of disseminated STRs.

Case Study : Bogus Contract Payments from Public Sector Undertaking

1. Suspicious Transaction Report

- The subject is a minor maintaining savings bank account operated by the mother and natural guardian.
- High value amounts credited in the account, mostly through transfer from several current accounts maintained at the same branch.
- Total credits aggregated to Rs. 8.27 Cr; No debits.
- Several accounts in the name of family members with similar transactions. Total credits Rs. 58.82 Cr.
- Several cheque deposits and multiple withdrawals in a single day.
- In all 8 linked STRs filed in the names of family members, mostly housewives.

2. Indicators of Suspicion

- Accounts in the name of minors with large value credits and little/no debits.
- Most accounts operated by natural guardian who were housewives.
- Multiple accounts with same bank/ branch with similar type of transactions.
- Transactions not commensurate with declared business activity of some of the account co-holders.
- Subjects residing in the coal belt.

3. Results of Investigation

- STR triggered enquiries by the Investigation wing of CBDT
- Enquiries revealed that the subject maintained accounts of 135 firms operated in the name of family members and close associates.
- No books of accounts maintained.
- No evidence of execution of contracts undertaken by the firms, as claimed.
- Source of deposits was misappropriated funds from a public sector undertaking on the basis of fake bills & bogus contract works.
- Search led to seizure of cash Rs.80 Cr., FDs Rs. 36 Cr, KVP Rs.12 Cr, Immovable property worth 20 Cr and investments in shares/MFs of Rs.80 Lac.
- Total value of seizure exceeded Rs 138 Cr.
- Matter also being investigated by CBI & Vigilance Department of the PSU.
- Enquiry by the PSU found that Rs 231 Cr had been paid during 2009-11 and 2011-12 to fake firms.

number of dissemination reports is higher than the number of STRs disseminated.

Two-way communication channels have been developed with the partner agencies, to receive feedback on the usefulness of intelligence reports disseminated. An understanding of the outcome of disseminated intelligence reports enables FIU-IND to enhance the analysis process as well as guide the reporting entities to improve quality of reporting.

Role of FIU-IND in Combating Financing of Terrorism (CFT)

A. Preventing misuse of the financial system

Financial institutions (reporting entities) are often the front-line defense against financing of terrorism and can contribute significantly by increasing vigilance against the abuse of the financial system. The regulators have issued detailed KYC/AML/CFT guidelines covering the

National ML/TF Risk Assessment

FIU-IND was actively involved in the National ML/FT Risk assessment as member of the inter-ministerial Committee set up by the Ministry of Finance in 2009.

The terms of reference of the committee covered:

(a) Money laundering and terrorist financing risks in lndia
(b) National AML/CFT strategy
(c) Institutional framework for AML/CFT
(d) Framework to measure the effectiveness of the strategy

The report on National ML/FT Risk Assessment was finalized in 2011. This report presents a consolidated national ML/TF risk assessment for the products and services in the Indian financial sector. The report included information on the following:

- Overview of money laundering, financing of terrorism and AML/CFT regime in India and existing mechanism for risk assessment and mitigation
- International activities and materials relevant to national risk assessment
- Methodology adopted by the committee in conducting this risk assessment
- Overview of the crime situation in India and threat assessment of various crime categories
- ML/FT methods and techniques used to disguise the criminal origin of the funds
- Relevant extracts of the STR Trend Analysis conducted by the FIU
- Risk assessment of various products and services in the Banking Sector, Securities Sector, Insurance Sector, Other Financial Institutions, Payment and Settlement and India Posts
- Institutional framework for AML/CFT in India
- Key elements of national AML/CFT strategy and framework for measuring the effectiveness of AML/CFT Strategy

The committee also made recommendations relating to mitigation of risks, implementation of risk based approach and effective assessment of risk

- Department of Revenue (DoR)
- Department of Economic Affairs (DEA)
- Ministry of Home Affairs (MHA)
- Enforcement Directorate (ED)
- Financial Intelligence Unit India (FIU-IND)
- Central Bureau of Investigation (CBI)
- Intelligence Bureau (IB)
- Directorate of Revenue Intelligence (DRI)
- Narcotics Control Bureau (NCB)
- Central Economic Intelligence Bureau (CEIB)
- Reserve Bank of India (RBI)
- Department of Posts
- Securities and Exchange Board of India (SEBI)
- Insurance Regulatory and Development Authority (IRDA)

areas of customer acceptance, customer identification, monitoring of transactions and risk management. Rigorous implementation of these guidelines by the reporting entities creates deterrence to use of legitimate channels for financing of terrorism. FIU-IND contributes to this aspect by increasing awareness of the reporting entities about their obligations under PMLA and monitoring their compliance.

B. Detection and reporting of suspected cases of financing of terrorism

Under the PMLA, every reporting entity is required to submit suspicious transaction reports (STRs) to FIU-IND. The definition of 'suspicious transaction' in the PMLA Rules was amended in May 2007 to specifically provide for reporting of suspect transactions relating to terrorist financing. The success of AML/CFT regime is critically dependent on the capability of the reporting entities in identifying and reporting suspicious transactions. FIU-IND has been actively involved in sensitizing reporting entities about their obligation to report STRs related to suspected cases of terrorist financing and providing guidance on detection and reporting of such transactions.

C. Information exchange with Domestic Agencies on suspected cases of financing of terrorism

One of the main functions of FIU-IND is to analyse and add value to the reports received from the reporting entities. Cases considered useful are disseminated to the law enforcement and intelligence agencies for appropriate action. As many STRs are found to be false positives due to partial matching of names, enhanced due diligence is conducted by FIU-IND. In addition, FIU-IND also supports the efforts of domestic intelligence and law enforcement agencies against terror financing by providing information specifically requested by them, either by searching its database or by calling specific information from the reporting entities***. Table7***

Table 7 - Requests received from Intelligence Agencies

Category	2008-09	2009-10	2010-11	2011-12	Till 31st March 2012
Requests received from intelligence agencies	190	226	428	473	1444

This table shows the number of references received from domestic intelligence agencies.

D. Information exchange with foreign FIUs on terrorism financing cases

FIU-IND was admitted as a member of the Egmont Group of FIUs in May, 2007. FIU-IND is regularly sharing information with foreign FIUs over Egmont Secure Web on suspected money laundering and terrorism financing cases. FIU-IND has MoUs with 19 countries and has also initiated the process to enter into MoUs with other foreign FIUs for furthering cooperation and exchange of information to combat money laundering and terrorist financing.

E. Contribution to global efforts to combat financing of terrorism

FIU-IND has been engaged through various fora to strengthen the international efforts to combat financing of terrorism. These include participation in various Working Groups of the Egmont Group, particularly Operational Working Group (OpWG) which seeks to bring FIUs together on typologies development and long-term strategic analytical projects and IT Working Group. FIU-IND also participates in the Joint Working Groups (JWGs) on Counter Terrorism set up by the Government of India with various countries.

F. Providing inputs to strengthen legal and operational framework to combat financing of terrorism

FIU-IND monitors latest trends and provides inputs for policy changes to strengthen the CFT regime in India. It also suggests mechanisms to increase effectiveness of the law enforcement agencies engaged in combating financing of terrorism.

Chapter 4

Domestic and International Cooperation - Building Partnerships

FIU-IND values its relationship with the financial sector and the law enforcement and intelligence agencies. FIU-IND serves as an important link between the two. At FIU-IND, emphasis is placed on understanding the needs of the enforcement and intelligence agencies and providing intelligence product that helps in fighting against money laundering and terrorist financing more effectively. Such relationships extend beyond mere dissemination of intelligence reports. FIU-IND expects the domestic agencies to continuously monitor the outcome of the FIU's input and provide feedback on its utility so that the reporting entities can be guided accordingly to refine their red flag indicators (RFIs) for generating alerts and report quality STRs.

During the year, FIU-IND continued to maintain close professional relationship with partner agencies based on mutual trust and understanding. FIU-IND is working on an effective information exchange module (FINex) as part of the Project FINnet which will not only ensure availability of information to the partner agencies but considerably enhance its ability to respond faster to the requirements of the agencies.

Workshops were held in which the framework of information exchange and various modules of the FINex were explained to the representatives of Law Enforcement Agencies and Intelligence Agencies. A demonstration of the functionality of the bulk request utility to generate XML and input XML was also given to the participants with sample data.

Law enforcement/ intelligence agencies

Timely dissemination of intelligence is an essential requirement of an FIU. FIU-IND constantly endeavours to process and analyse the STRs in the shortest possible time considering the resources available. FIU-IND believes in supporting the efforts of law enforcement and intelligence agencies in combating money laundering and financing of terrorism, through timely dissemination of intelligence reports. FIU-IND also provides them with additional financial information available in its databases, on request.

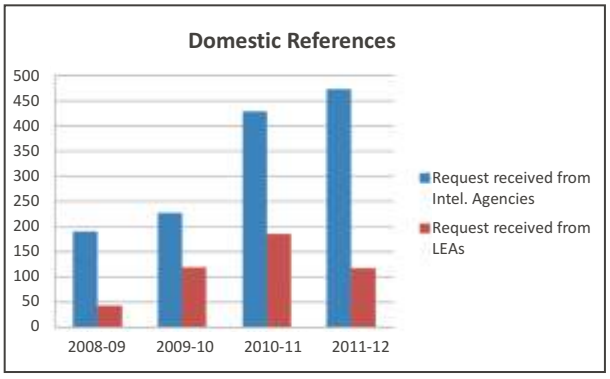
In order to enhance the operational relationships with the partner agencies, FIU-IND has appointed nodal officers to deal with all issues relating to individual agencies. This has augmented the effectiveness of the structured interactions and enhanced the quality of understanding with agencies. Meetings were organized during the year with the nodal officers of the law enforcement and intelligence agencies for better coordination and for sensitizing them about the manner in which FIU-IND information is to be handled.

FIU-IND actively participated in meetings of Central Economic Intelligence Bureau (CEIB) and Regional Economic Intelligence Councils (REICs) to discuss issues of common interest. FIU-IND also interacted with the nodal officers of law enforcement agencies of the state governments and union territories.

FIU-IND's databases on cash and suspicious transactions are found very useful by domestic law enforcement and intelligence agencies. The partner agencies relied on information contained in FIU-IND databases not only for developing intelligence but also for strengthening ongoing investigations. During the year, FIU-IND provided timely information to various agencies in response to 590 references on money laundering, terrorist financing, corporate frauds, organized crimes, fake Indian currency, tax evasion etc. ***Table 8***

Table 8: No. of references from domestic law enforcement /intelligence agencies

Category	2008-09	2009-10	2010-11	2011-12	Till 31st March 2012
Requests received from intelligence agencies	190	226	428	473	1,444
Requests received from law enforcement agencies	42	118	186	117	476



The details of interactions with law enforcement and intelligence agencies during the year are at ***Appendix G***.

FIU-IND initiated the practice of entering into Memorandums of Understanding (MoUs) with partner agencies in order to provide a structural framework for enhanced cooperation and understanding. FIU-IND has signed MoU with three partner agencies, namely Enforcement Directorate, Central Board of Direct Taxes, and Central Bureau of Investigation. MoUs are also being negotiated with other partner agencies. It is also planned to have similar MoUs with the regulators of financial sector (RBI and SEBI).

Regulators

FIU-IND has developed close relationship with financial sector regulators for strengthening AML and CFT regulations. The regulators, namely, Reserve Bank of India (RBI), National Bank for Agricultural and Rural Development (NABARD), Securities and Exchange Board of India (SEBI) Insurance Regulatory Development

Authority (IRDA) and National Housing Bank (NHB) have issued instructions to the financial sector entities for adherence to KYC, AML and CFT norms. FIU-IND has ensured that suitable modifications are carried out in the circulars, wherever necessary. These circulars are also uploaded on the website of FIU-IND for quick reference.

FIU-IND continued its regular interaction with regulators, industry associations and Self Regulatory Organisations to develop a common understanding of obligations under PMLA, and improve compliance with AML norms and reporting obligations under PMLA. FIU-IND also interacted with regulators for identification of legal provisions requiring amendment, issues requiring clarification/intervention and for developing indicators for industry specific suspicious transactions. Sector-specific issues were identified from trend analysis of STRs and shared with concerned regulators for requisite intervention.

FIU-IND assists regulatory authorities in training their staff to improve their understanding of AML/CFT issues. This helped them in monitoring the effectiveness of AML systems of institutions inspected by them.

Global AML/CFT efforts

Money Laundering and terrorist financing techniques evolve quickly, presenting new threats to our financial systems. We live in an increasingly interconnected world and money launderers will exploit any gaps between countries. For this reason we must have a global solution to a global challenge. FIU-IND contributed in the efforts of the international community by adopting a strategy of building healthy relationships based on trust and cooperation with its counterpart FIUs of other countries. During 2011-12, there was a significant increase in spontaneous sharing of information. Four MoUs were signed during the year with FIUs of Israel, Poland, Singapore and Nepal. Many more MoUs are under negotiation with other FIUs. FIU-IND continued to contribute in the activities of regional and international bodies dealing with AML/CFT issues.

Officials from Royal Monetary Authority (RMA) of Bhutan visited FIU-IND in June, 2011 to seek technical assistance for establishing a reporting system for FIU Bhutan. The officials discussed the way forward to help Bhutan develop suitable application for their reporting system. A team consisting of an Additional Director and Technical Director from FIU-IND visited Bhutan in November 2011 to assess and advise Royal Monetary Authority of Bhutan on the technical infrastructure requirements for setting up an FIU in Bhutan.

In September, 2011 an Additional Director of FIU-IND visited FIU of Mauritius for assessment of their technical infrastructure and provide assistance in strategic planning. The assessment exercise was based on the **FIU Information System Maturity Model (FISMM)**, which is being developed by the Egmont Group of FIUs and in which FIU-IND is playing a lead role. FISMM is a comprehensive framework to enable FIUs of different sizes to assess the maturity level of their processes and IT systems. The maturity assessment of the FIU of Mauritius was conducted and domains requiring improvement were identified. The exercise helped in preparing a strategic plan with short term and medium term goals. A workshop was held with the analysts of the FIU of Mauritius to provide hands-on training on strategic analysis.

While attending FATF plenary from 21-28 October, 2011, at Paris, the Director, FIU-IND signed an MoU on exchange of information with FIU of Singapore.

Signing of MoU with Singapore

Following this MoU, Singapore FIU-IND has shared important information relating to some of the ongoing cases of investigation by domestic agencies. Director also held courtesy meetings with his counterparts from Mauritius, Hong Kong, China and Russia on the margins of the Plenary. Delegation from Bangladesh expressed interest in signing an MoU with India.

FIU-IND and FIU of Nepal signed an MoU in November 2011 to enhance cooperation and formalize exchange of information of cases relating to money laundering and related crimes between the two FIUs.

FIU-IND has been participating in the meetings of Contact Group on Piracy off the coast of Somalia (CGPCS). CGPCS presently operates through four working

FIU Information System Maturity Model (FISMM)

Overview

FIU Information System Maturity Model (FISMM) is a comprehensive framework developed by the Egmont Group to enable FIUs of different sizes in capability assessment, strategy formulation, performance management, process improvement, and technology evaluation in FIU environment.
FIU-IND played a pioneer role in development of this framework by preparing the project concept note in 2009 and leading the project with active involvement of other members of the Egmont Group.

FISMM Architecture
The FISMM framework has two dimensions, called "Domain" and "Maturity level" to clearly segregate basic characteristics of the key domains from its institutionalization characteristics.
The domain dimension of the model covers all main domains or process areas in FIU environment. The prefix FD in domain code stands for FISMM Domain. The domains FD01 to FD11 are FIU specific whereas domains FD12 to FD15 cover IT implementation in general. Each domain in FISMM includes base practices which must be successfully implemented to accomplish the purpose of the domain they support. Under each base practice of the domain, the description of the base practice, example work products, and notes (covering related best practices) have been mentioned.
The maturity level for the domain is based on adoption of base and best practices in terms of coverage (i.e. whether practices are followed) and maturity level (i.e. whether activities are performed in adhoc manner or processes are monitored and measured).

Figure: FISMM matrix

Domain	Maturity Level 1	Maturity Level 2	Maturity Level 3	Maturity Level 4	Maturity Level 5
FD01 - Collection of reports					
FD02 - Access to information					
FD03 - Processing of information					
FD04 - Detection of new targets					
FD05 - Operational analysis					
FD06 - Strategic analysis					
FD07 - Domestic Cooperation					
FD08 - International Cooperation					
FD09 - Registration of reporting officer					
FD10 - Capacity building of reporting entities					
FD11 - Managing compliance of reporting entities					
FD12 - Performance management					
FD13 - Information management					
FD14 - Technical infrastructure management					
FD15 - Information security management					

Uses of FISMM

FISMM presents a framework to assess the various stages of process maturity and implementation of information system to evolve from an adhoc, less organized, less effective state to a highly structured and highly effective state. This model provides a guide to assist FIUs in:

- "Capability assessment" to assess maturity level of various domains
- "Strategy formulation" to prioritise future initiatives
- "Performance management" to measure the performance of various functions
- "Process improvement" to design new processes or improve process capability
- "Technology evaluation" to evaluate and select suitable technology

Figure: Uses of FISMM

Figure: Sample Capability Assessment result using FISMM

	Maturity Level 1	Maturity Level 2	Maturity Level 3	Maturity Level 4	Maturity Level 5
FD01 - Collection of reports	■	■			
FD02 - Access to information	■	■	■		
FD03 - Processing of information	■				
FD04 - Detection of new target s					
FD05 - Operational analysis	■	■	■		
FD06 - Strategic analysis					
FD07 - Domestic Cooperation	■	■	■		
FD08 - International Cooperation	■	■	■		
FD09 - Registration of reporting officer	■	■			
FD10 - Capacity building of reporting entities	■	■			
FD11 - Managing compliance of reporting entities	■				
FD12 - Performance management	■	■			
FD13 - Information management	■	■			
FD14 - Technical infrastructure management	■	■			
FD15 - Information security management	■	■	■		

Future Roadmap

The FISMM text relating to base practices (example work products, related best practices) and technology (required functionalities, products, technologies) needs to be regularly updated to reflect the changes in the operating environment, emerging work practices and new technologies. The Egmont Group has set up a governance structure including an FISMM subgroup to manage and update the FISMM document.

groups. They have formed Group-5 to track financial aspects of piracy and to co-ordinate efforts to disrupt maritime piracy by targeting the financial network of the pirates.

The objective of the meetings has been to build capacity of FIUs and Law Enforcement Authorities to counter ML through tracking movement of ransom money and to promote international cooperation in the area of information sharing and prosecutorial assistance. Financing of maritime piracy and the flow of the ransom money are still matters of research and organizations like the World Bank, UNODC and INTERPOL are analyzing and linking various piracy incidents and also compiling data on pirate groups, individual pirates, their financiers, investors and profiteers of piracy with a view to understand the entire financial flow related to Somali Piracy. The 2nd Ad-hoc meeting on financial aspect of piracy held in Seoul, South Korea on 29th June,2011 and the first meeting of Working Group 5 of the contact group on Somali Piracy held in Italy on 7th October,2011 were attended by an officer of FIU-IND .

Financial Action Task Force

The Financial Action Task Force (FATF) is an inter-governmental body that works for the development of standards for combating money laundering and terrorist financing. It assesses and monitors the progress made by its member countries in the areas of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

In February, 2012, FATF has issued the revised International Standards on Combating Money Laundering and Financing of Terrorism and Proliferation. In the new recommendations, the earlier 9 Special Recommendations relating to terrorist financing have been merged with the general recommendations and the coverage of the recommendations has been extended to proliferation financing. The revisions seek to address new and emerging threats, clarify and strengthen many of the existing obligations, while maintaining the necessary stability and rigour in the Recommendations. The new standards also allow countries to apply a "Risk-Based Approach", within the framework of the FATF requirements, thereby permitting adoption of a more flexible set of measures, in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way. A summary of the revised FATF Recommendations relevant to the FIU and the reporting entities is given at ***Appendix-H***.

India is one of the 34 member jurisdictions and 2 regional organizations (European Commission and Gulf Co-operation Council) that are the FATF members.

FIU-IND has actively participated in the activities of the Financial Action Task Force (FATF). Officers from FIU-IND were a part of the Indian delegation to FATF and attended the FATF meetings in September 2011 at Rome, Italy and in October 2011 and February 2012 at Paris, France.

FATF Style Regional Bodies (FSRBs)

There are 8 FSRBs which provide leadership in their regions and are an important means of promoting consistency in application of the FATF standards. India is a member of 2 FSRBs, the 40-member Asia Pacific Group (APG) and the Eurasian Group (EAG). India's joining EAG in December, 2010 will strengthen the regional cooperation in combating money laundering and the financing of terrorism. FIU-IND has been an active participant in the activities of APG and EAG.

A workshop was organized by the World Bank jointly with the Eurasian Group (EAG) at Kiev, Ukraine on 21st and 22nd April, 2011 which was attended by an Additional Director from FIU-IND. The workshop, which was attended by delegations from eight Countries, discussed issues related to latest revision of FATF recommendations and adoption of risk-based approach/ risk assessment exercise carried out by their countries. Besides, FIU-IND was also represented in the Indian delegation to the Eurasian Group (EAG) Plenary and its

Working Group Meetings at Moscow in June 2011 and at Xiamen, China in November, 2011.

FATF Mutual Evaluation Report 2010

Financial Action Task Force (FATF) carried out a mutual evaluation of India in 2009 and 2010. The Mutual Evaluation Report (MER) of FATF, released in June 2010, rated India as partially complaint (PC) and non-compliant (NC) on 19 recommendations. Five core and key recommendations were rated as PC. None of the core and key recommendations was rated as NC. A summary of ratings is given at ***Appendix I.***

Recommended Action for FIU-IND

With regard to the FIU-IND, the actions suggested in the MER are listed in ***Table No.9.***

Summary of Action taken by FIU-IND

Based on the findings of MER, FIU-IND drew up an Action Plan to be implemented in the short-term (before 31.03.2011) and medium-term (before 31.03.2012). The action taken on the specific suggestions of FATF are listed in ***Table No. 10.***

Table 9: Action suggested in MER 2010.

Recommendation	Action suggested in MER
R 12, R 16, R 24 (Designated Non-Financial Businesses & Professions)	• Compliance of FATF standards by Casino Sector. • Greater outreach programme for professional bodies like Bar Council, ICAI and ICSI.
R13, SR IV (Suspicious transaction reporting)	• Comprehensive review of adequacy of STRs relating to different sectors, geographies and proceeds of crime. • Comprehensive review of adequacy of STRs related to terrorist financing (TF). • Focused outreach to train reporting entities in detecting TF related STRs. • Review of existing circulars/guidance related to detection and reporting of TF related STRs.
R 26 (Financial Intelligence Unit)	• FIU-IND to enhance its capability in relation to intelligence and information dissemination. • FIU-IND to publish a report on trends and typologies on annual basis.

FATF on-site visit

A technical team of the FATF visited India during 11-18 April 2011. The review team's overall impression was that India is strongly committed to the FATF process and to the implementation of an effective AML/CFT framework.

With regard to the functioning of FIU-IND, the FATF team commented in its report that *"The FIU is to be commended on the efforts that it has made over the past year to pick up on the points made in the MER, to monitor the trends in STR filing, and to be proactive in its direct engagement with the reporting institution".*

The FATF on-site team also acknowledged that the FIU is well advanced in the development of its FINnet system, which will provide for real-time filing of STRs by all reporting institutions. Once fully-implemented, the team observed, the system is intended to enhance the efficiency and quality of reporting and the analytical capabilities of the FIU.

The FIU has also undertaken extensive outreach to the financial institutions by way of seminars and training workshops, which have included special programmes on terrorist financing. In the past year, FIU personnel have participated in 50 such projects involving over 2000 attendees, and have also run a train-the-trainer course for 57 staff from the country's bank training colleges. The FIU has also undertaken focused reviews of compliance with the STR requirements by both the public and private sector banks. The effect appears to have been a markedly improved reporting regime.

Egmont Group of FIUs

The Egmont Group of FIUs promotes international cooperation and free exchange of information among all FIUs. The Egmont Group aims to provide a forum for FIUs to improve understanding and awareness of issues and an opportunity for enhancement of their capacities to develop intelligence to combat money laundering and terrorist financing.

Table 9: Summary of Action Taken by FIU-IND

Recommendation	Action taken by FIU-IND
R 12, R 16, R 24 (Designated Non-Financial Businesses & Professions)	• A Casino Sector Assessment Committee (CSAC) was constituted under the chairmanship of Director (FIU-IND) which carried out a comprehensive review of the Casino Sector. The Committee has made several recommendations to the Government for strengthening the AML/CFT regulatory framework for this sector including- ▪ Creation of comprehensive legal framework. ▪ Autonomous regulators or Gaming Commissions for casinos. ▪ Cooperation between regulators of different States. ▪ Effective 'fit and proper' test. ▪ Review of current KYC threshold to align it to FATF standards. ▪ Issue of comprehensive AML/CFT guidelines. • Several outreach programmes were conducted by FIU-IND for ICAI and ICSI during August 2010- March 2011, which were attended by 230 Chartered Accountants and 558 Company Secretaries. • FIU-IND approached ICAI, ICSI and ICWA for inclusion of modules on AML/CFT in the curriculum of their courses and offered assistance and guidance in updating the course contents. • A training workshop on Combating Financial Crime was organized by the Institute of Company Secretaries of India (ICSI) in March 2012, which was addressed by a senior officer of FIU-IND. • FIU-IND officers conducted another outreach programme with the Institute of Chartered Accountants in June, 2012, which was attended by 54 participants. The participants were given exposure to the international AML/ CFT standards and the AML/CFT regime in India along with inputs on methods to
R13, SR IV (Suspicious transaction reporting)	• FIU-IND has, in consultation with RBI and IBA, identified red flag indicators to detect suspected TF cases. • An analysis of the adequacy of STRs related to different sectors and geographies was carried out by FIU-IND. • A special review of AML compliance level by the private sector banks has been done by FIU-IND and 11 banks have been identified for close monitoring of their reporting system. • Advisories have been issued to 323 Reporting Entities during 2010-11 for improvement in number and quality of reporting. • Penalties have been imposed on two banks for failure to put in place a satisfactory system for identification and reporting of suspicious transactions. • FIU-IND has been encouraging the reporting entities to conduct in-house training on AML/CFT for their own employees. Feedback received from 31 training colleges of banks, which attended the "Train the Trainer Workshop" held on 29.9.2010, shows that these colleges have conducted 1,981 training programmes on AML/CFT, attended by 59,267 bank employees. 1,896 of such training programmes included a specific module on Terrorist Financing. • FIU-IND is in dialogue with Indian Institute of Banking & Finance (IIBF) for expanding outreach in the banking sector. IIBF has been conducting a certificate course in "Anti Money Laundering and KYC Guidelines" since 2005 and 13,031 candidates have been given certificates. • The number of TF related STRs has increased in 2010-11 to 259, which is a 100% increase over 2009-10 figures. • An analysis of the adequacy of STRs related to different sectors and geographies has been completed by FIU-IND based on the data of STRs received up to March 2010. The final report has been published by FIU-IND. • A special review of AML compliance level by the private sector banks has been done by FIU-IND and 11 banks have been identified for close monitoring of their reporting system. • Advisories have been issued to 323 Reporting Entities during 2010-11 (as against 237 in 2009-10 and 214 in 2008-09) for improvement in number and quality of reporting. • Penalties have been imposed on two banks for failure to put in place a satisfactory system of identification and reporting of suspicious transactions. • A Working Group consisting of select banks along with RBI, IBA and FIU-IND was formed to help banks to evolve common platform/practices in dealing with KYC/AML related issues under PMLA, 2002 and suggest standard parameters for all banks to generate suspicious transactions. The Working Group submitted its report in March 2011 which has been circulated to banks vide IBA's circular dated May 18, 2011 for information and implementation. • Several rounds of meetings have been held with the intelligence agencies to assess the effectiveness of STRs related to Terrorist financing and identify red flag indicators to detect suspected TF cases.

Table 9: Summary of Action Taken by FIU-IND

Recommendation	Action taken by FIU-IND
R 26 (Financial Intelligence Unit)	• A report on trends of STRs has been compiled and published. • FIU-IND has held regular meetings with nodal officers of central law enforcement agencies and state police. • FIU-IND conducted several training sessions covering 'AML/CFT regime and role of FIU-IND' for officers of central and state law enforcement agencies. • FIU-IND organized an interactive session with representatives of the law enforcement and intelligence agencies to present the implementation roadmap of Project FINnet • FIU-IND participated in five training programmes organized by the CBI Academy and the National Academy of Customs Excise and Narcotics (NACEN) on a range of AML related topics which was attended by around 138 officers of central and state law enforcement agencies. • FIU held meetings in five state capitals to interact with the senior officers of state police. The interactions have further strengthened the mechanism for information sharing. • FIU-IND held 3 meetings with the intelligence agency and the law enforcement agency, to whom the largest number of STRs are disseminated, to apprise them of the progress in the implementation of Project FINnet and to explain the role and responsibilities of the agencies under the new system. • During 2011-12, 34 trainings were organized for the law enforcement authorities on various issues of AML/ CFT, which were attended by 1,422 officers of these agencies.

The membership of Egmont Group has increased to 131 as on 31st March 2012. Member FIU undertake to subscribe to the Egmont Group principles. FIU-IND was admitted as a member of the Egmont Group at the Bermuda Plenary session in May 2007. During the month of June 2007, Egmont Secure Web (ESW) was also made operational for exchange of information over a secure network.

Officers of FIU-IND participated in the 19th Annual Plenary session of Egmont Group at Yerevan, Armenia in July 2011 and the Egmont Working Group at Manila in Philippines in January/February 2012. FIU-IND Officials have been actively participating in Operational Working Group (OpWG), Training Working Group (TWG) and IT Working Group (ITWG). The most significant contribution of FIU-IND in ITWG has been to the development of **FIU Information System Maturity Model (FISMM).** During the Egmont Group Plenary held at Yeravan, Armenia in July, 2011 the representatives of the Operational Working Group (OpWG) and Training Working Group(TWG) reviewed the FISMM document and provided feedback on the domains, goals, indicators , etc. During the WG meetings at Manila, the ITWG and OpWG discussed the peer review result and expressed their interest in taking the project forward and decided to seek approval of the HoFIUs in the 20th Egmont Plenary at St. Petersburg in July 2012. Leadership in FISMM project gives FIU-IND an important role in defining the emerging standards for assessment of effectiveness of FIUs.

FIU-IND continued to be the one of the two regional representatives of the Asia group, along with Qatar, in the Egmont Committee. The Director, FIU-IND presented the regional review report as Asia representative in Egmont Committee.

A Charter Review Project (CRP) team was set up in July 2011, to review the "Egmont Group Charter of 2007 and Associated Documents" in light of the revised FATF Standards. The Egmont Charter is being reviewed for the first time after the establishment of the Egmont Group in 1995. The Project is headed by the Chair of the Egmont Group (Belgium) and has two streams i.e. Legal and Corporate. The Legal stream is responsible for the Egmont standards, principles and best practices while the Corporate stream is responsible for the governance issues, including the Egmont Group structure, functions

and responsibilities of the Egmont Committee, the Secretariat, the working groups, and the regional representatives, etc.

Director, FIU-IND is a member of the Legal stream (headed by Italy) and has been assigned 3 out of 18 issues (Analysis Function, Data Protection & Confidentiality and Channels of Information Exchange) identified for detailed examination. This has given FIU-IND the unique opportunity of participating, for the first time, in the standard setting process of the Egmont Group. In this process, FIU-IND has contributed detailed papers on all the three issues assigned to FIU-IND and also provided substantive comments on the other issues dealt with by the other countries. The Director attended intersessional meeting of the CRP held in Paris on 21st Oct, 2011.

The Egmont Working Group and Committee Meetings, held in Manila, Philippines from 30 Jan. 2012 to 03 Feb. 2012 were attended by the Director and two other officers of FIU-IND. The Director took part in the deliberations of 'Egmont Group Charter Review Project' as a member of legal group. A paper on the peer review on the FISMM project was presented.

An Additional Director from FIU-IND facilitated a session on “Securing an FIU” during Joint APG/Egmont Group FIU Seminar held at Busan, Korea on 9th Dec. 2011, as part of an ongoing project. The one day seminar was intended to discuss best practices in the area of enhancing FIUs security and operational efficiency. India is one of the contributors of the best practice guide being prepared on Information Security in FIUs.

Co-operation and exchange of information with other FIUs

FIU-IND adheres to the Egmont principles of free exchange of information. All requests for information are replied to, in time, including cases where no information could be found.

The statistical information regarding number of cases in which requests were made by FIU-IND to other FIUs and number of cases where FIU-IND received requests from other FIUs is in ***Table 11***.

Table 11 - MoUs with Foreign FIUs

FIU & County	MoU signed on
Israel Money Laundering Prohibition Authority (IMPA), Israel	12.07.2011
General Inspector of Financial Information, Poland	12.07.2011
Suspicious Transaction Reporting Office (STRO), Singapore	24.10.2011
Financial Information Unit, Nepal	17.11.2011

FIU-IND does not require an MoU with foreign FIUs for exchange of information, and can do so on the basis of reciprocity. However, in order to enhance the level of co-operation and to provide a structured framework for better understanding, FIU-IND continued the process of entering into a MoUs with various FIUs during the year. MoUs with the FIUs of Israel, Poland, Singapore and Nepal were signed during the year. MoUs with more than 20 countries are under various stages of negotiation.

Joint Working Groups on Counter Terrorism

In order to enhance the level of cooperation on various operational issues relating to terrorism and other crimes including money laundering and drug trafficking, India has set up Joint Working Groups with various countries. FIU-IND regularly participated in these Joint Working Groups as member of Indian delegations.

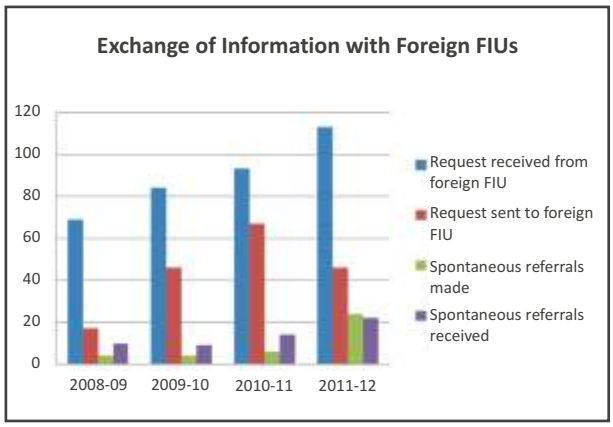


Table 10 - Exchange of Information with Foreign FIUs

Status of action Taken	2008-09	2009-10	2010-11	2011-12	Till 31st March 2012
Request received from foreign FIU	69	84	93	113	412
Request sent to foreign FIU	17	46	67	46	191
Spontaneous referrals made	4	4	6	24	42
Spontaneous referrals received	10	9	14	22	60

Chapter 5

Raising awareness and building capacities of reporting entities

The entities in the financial sector that have reporting obligations under the PMLA are referred as reporting entities. At present these include banking companies, financial institutions (insurance companies, housing finance companies, non-banking finance companies, chit fund companies, payment system operators, authorised money changers and casinos) and intermediaries of securities market. The number of entities operating in the financial sector in India is very large and it is a challenge to engage them and make them comply with the reporting obligations. The success of an FIU depends largely on the ability of reporting entities in effectively identifying and reporting transactions. FIU-IND continued its focus on increasing awareness of the reporting entities about their reporting obligations under PMLA and building their capacities to ensure better compliance.

A significant step taken in enabling the reporting entities to efficiently identify suspicious transaction and report to FIU was prescribing a standard set of Red Flag Indicators (RFIs) for the banking sector in July, 2011 in collaboration with RBI and IBA. On the same lines Working Groups were formed for payment system operators and money transfer service providers. The exercise will;

- Create a common and shared understanding aligned with global norms and practice about the implementation of STR detection and reporting systems.

- Provide indicative lists of high risk customers, products, services and geographies.
- Provide a list of commonly used alert indicators for detection of suspicious transactions.
- Provide guidance for an effective alert management and preparation of STRs.

As in earlier years, FIU-IND adopted a multi-pronged strategy to enhance awareness through the FIU's website, seminars and workshops. FIU-IND supported the regulators, industry associations, professional bodies and reporting entities by providing resource persons for seminars and workshops organized by them. A 'Train the Trainers' workshop is organized by FIU-IND every year to create master trainers. Training material prepared by FIU is being made available to all reporting entities to conduct their own training seminars. The master trainers in turn conducted several AML/CFT focused seminars and workshops in their organisations.

FIU website

The FIU-IND website (http://fiuindia.gov.in) is a user-friendly site containing information on AML/CFT issues including PMLA and its amendments, rules and regulations, relevant circulars and instructions issued by regulators and reporting formats. FIU-IND has also developed software utilities for submission of reports in electronic format for use by the smaller reporting entities that have limited IT infrastructure. These utilities are available for free download on the FIU-IND website.

Seminars and workshops

During the year, FIU-IND participated in 42 workshops/interactions on AML/CFT awareness in collaboration with regulators, industry associations, professional bodies and reporting entities, targeted at over 2,500 participants. The statistics relating to training seminars and workshops are in ***Table 13.***

During the year, FIU-IND continued its focus on enhancing awareness among Authorized Dealers/Full Fledged Money Changers (FFMCs) and Money Transfer Service Scheme (MTSS) operators and their agents who were inducted as reporting entities recently.

Eight review-cum-training programs were conducted for the CEOs/Chairmen/Principal Officers of the Cooperative Banks comprising Urban Cooperative Banks(UCBs), District Central Cooperative Banks(DCCBs) and State Cooperative Banks(SCBs) covering 804 officers.

Table 13: Outreach Activities

Outreach Activity	Number of Interactions				
	08-09	09-10	10-11	11-12	Till 31.3.12
Seminars and Training workshops	103	76	50	42	421
Number of Participants	3,617	3,145	2,264	2,509	19,763

The details of outreach activities conducted during the year are at ***Appendix I.***

'Train the Trainers'

A 'Train the Trainers' workshop was organized by FIU-IND in September 2011 at India Habitat Center, New Delhi. This workshop is organized once every year with the objective of increasing the availability of in-house trainers among reporting entities. This program was attended by 47 key resource persons and trainers of banks, training Institutions, Regulators and Department of Post. The program was inaugurated by the Finance Secretary & Revenue Secretary and was addressed by officers from FIU-IND and speakers from SBI, RBI and ICICI. The workshop has been effective and popular and similar workshops are planned for the coming years.

Feedbacks received from the banks suggests that the Train the Trainer program has been quite successful in spreading awareness levels of the AML teams of the banks through the trained resource persons and material supplied during the program. Some banks have made AML/CFT course a mandatory training for all their employees.

Finance Secretary addressing the participants of 'Train the Trainers' program, 2011

Participants at the 'Train the Trainers' program, 2011

Chapter 6

Ensuring Compliance with reporting obligations under PMLA

Compliance with reporting obligations under AML law is one of the major challenges faced by FIUs. FIU-IND's strategy to ensure compliance by reporting entities is multi-pronged. While FIU-IND has been focusing on raising awareness of AML/CFT in the financial sector through workshops and seminars organized for the employees of the reporting entities in association with Regulators, and Industry Associations, it has also been regularly conducting review meetings with Principal Officers of the reporting entities to provide guidance and feedback on their reports.

Review meetings

FIU-IND has been undertaking periodic sector-wise reviews to evaluate the AML performance in specific sectors ***(Table 14)***. These review meetings are held with principal officers of reporting entities. The representatives of regulators and industry associations such as Indian Banks Association, Life Insurance Council and AMFI were invited to participate so that industry-specific issues could be discussed in detail, and a common understanding of issues could develop across a sector. Sector-specific meetings helped FIU-IND to evaluate the AML performance of individual reporting entities as compared with their peers, and to enable individual reporting entities to benchmark their performance.

During the sector review meetings, the number and quality of reports submitted by individual reporting entities were analyzed to assess gaps and identify focus areas for individual entities that were not performing against the benchmarks set by their peers. Examples of sanitized cases and feedback

Table 14 -Review Meetings with Principal Officers

Month	Meetings held with
April 2011	▪ Public Sector Banks
May 2011	▪ Public Sector Banks
June 2011	▪ Indian Private Sector Banks ▪ Public Sector Banks
July 2011	▪ Indian Private Sector Banks ▪ Public Sector Bank
August 2011	▪ Indian Private Sector Banks ▪ Public Sector Banks ▪ Life Insurance Council
September2011	▪ Public Sector Bank s ▪ Indian Private Sector Banks
October2011	▪ Public Sector Bank Money Changer Association
November2011	▪ Association of Mutual Funds of India ▪ Private Institutions ▪ Public Sector Banks
December2011	▪ Indian Private Sector Banks ▪ Public Sector Banks
January2012	▪ Indian Private Sector Banks
February2012	▪ National Federation of Cooperative Banks ▪ Life Insurance Companies ▪ IRDA
March 2012	▪ Indian Banking Assaociation ▪ RBI ▪ Public Sector Banks ▪ National Federation of Urban Cooperative Banks

received by FIU-IND from law enforcement and intelligence agencies were also shared during these meetings.

Other compliance measures

FIU-IND has a compliance section to act as nodal point for enforcing compliance and for corrective action in cases of non-compliance. The compliance section monitored submission of reports, data quality in reports as well as infrastructure issues such as strength of AML team, status of computerization and installation of AML software, etc. Information emerging from investigations conducted by law enforcement agencies was also used to identify suspected cases of non-compliance with reporting obligations. Information culled out from STRs was also used to examine if other reporting entities had also examined and reported these transactions. Advisories were issued to reporting entities on problem areas suggesting corrective action. Reporting entities suspected of lagging behind were selected for review on the basis of comparison of their performance with peers. The performance of these selected entities was monitored during the year, to assess if their performance showed improvement or whether further interventions were required.

During the year, 938 advisories were issued to reporting entities highlighting problem areas and advising them to improve their compliance under PMLA. During the year, in one case the fine imposed by FIU-IND was upheld by the PMLA Tribunal and the party has filed appeal before the Delhi High Court. The details of advisories issued are as under:

Table 15- Sector-Wise Statistical Analysis of Advisories issued

Sl. No	Category	2009-10	2010-11	2011-12	Total
1	Public Sector Banks	24	23	8	100
2	Indian Private Sector Banks	15	29	7	84
3	Foreign Private Sector Banks	3	33	0	65
4	Regional Rural Banks	12	22	800	878
5	Urban Co-operative Banks	150	206	82	489
6	Capital Market Intermediary	31	3	20	57
7	Insurance Companies	0	1	14	24
8	Other Financial Institutions	2	6	7	15
	Total	**237**	**323**	**938**	**1712**

Table 16-Subject-Wise Statistical Analysis of Advisories issued

Sl. No	Subject	2009-10	2010-11	2011-12	Total
1	CCR	79	59	0	216
2	CTR	126	249	0	470
3	STR	20	13	56	126
4	KYC/AML	0	0	0	3
5	Multiple issues	12	2	882	897
	Total	**237**	**323**	**938**	**1712**

FIU-IND's Strategy for ensuring compliance to PMLA

1. Increase voluntary compliance through increasing awareness:
   a. Raise awareness through outreach programs organized by Regulators, Industry Associations as well as individual reporting entities
   b. Encourage professional institutes to offer courses and training programs on AML/CFT, and provide resource persons for such courses
   c. Organize training programs for in-house training faculty of large reporting entities and regulators, so that their training institutes can supplement FIU-IND's efforts of increasing awareness
   d. Encourage reporting entities to organize regular refresher training courses for their employees
   e. Increase awareness about high risk scenarios and patterns that have been detected by law enforcement agencies and intelligence agencies
2. Ensure adherence to reporting obligations by regular review meetings
   a. Conduct regular sector-specific meetings in coordination with sector regulator
   b. Identify reporting entities requiring a special attention and conduct individual meetings with these reporting entities
   c. Involve the senior management in the review process and sensitize them about their obligations
   d. Provide regular feedback to reporting entities about the quality of their reporting and problem areas requiring attention
3. Detect instances of contravention of reporting obligations
   a. Collect information on suspect instances of contravention of PMLA identified in investigations conducted by law enforcement agencies
   b. Where transactions involve a number of financial sector entities, and transactions are reported by one reporting entity, examine if the other reporting entities involved in the transactions have detected, examined and reported the transactions
   c. Through a risk-based approach, and through comparison with peer performance, identify the reporting entities requiring a detailed review or an onsite inspection
4. Adopt a graded system of imposing sanctions in case of contraventions
   a. Advise the reporting entities about the possible gaps identified, and the possible contravention suspected, and provide them an opportunity to rectify the mistakes. Provide guidance on the measures required to be implemented to plug the gaps identified
   b. Warn the reporting entity of the detected instance of non-compliance and advise on measures required to ensure compliance
   c. In cases of continued or serious contraventions, issue show cause notice for imposition of fine under Section 13 of PMLA, and impose fine on the reporting entity
   d. Continue to monitor the performance of the reporting entity for six months to one year to ensure demonstrated adherence to compliance

Chapter 7

Organizational Capacity Building

With new products and services offered by the financial sector, the money launderers keep developing new techniques to evade detection. FIU-IND analysts have to keep developing their skills to remain effective. FIU-IND believes in building strong organizational capacity to enhance its ability to identify and meet new challenges posed by money launderers and criminals in the dynamic and ever-changing world of crime.

With a view to enhance the capacity of its officers and to impart to them the knowledge of various sectors of the financial system in India, FIU-IND has taken the initiative to collaborate with some premier training institutes for targeted training relating to various financial sectors, financial instruments, sector-specific laws and regulations, financial crimes, regulatory framework, etc.

Regional Workshop organized by AUSTRAC at Kathmandu, Nepal in April, 2011

In this regard, efforts are being made to partner with the National Institute of Banking and Finance, Pune, the National Insurance Academy, Pune, and the National Institute of Securities Markets, Mumbai, for developing a course module for the FIU-IND officers of the duration of 2-3 weeks. All the three institutes have agreed to conduct a course and FIU-IND is in the process of working out the detailed modalities with the respective training institute.

Training is one of the tools to equip people with necessary skills. FIU-IND has made proactive efforts to regularly upgrade the skills of its employees by providing them opportunities for training on AML/CFT and related economic issues. During the year, FIU-IND officials attended training in different areas ***(Table17)*** including securities markets, commodity markets, corporate frauds, abuse of charitable and non-profit organizations, financial sector supervision and AML policy development

Table 17: Capacity building workshops attended by officers from FIU-IND

Month	Workshop	Organized by	Place
May 2011	Training Program on Prevention of Insurance Frauds	National Insurance Academy	Pune, India
June 2011	Joint India IMF Training Program on AML/CFT.	Jointly by RBI and IMF	Pune, India
June 2011	Training Program on Banking Operations and Fiscal Laws Enforcement	CEIB	State Bank Staff College, Hyderabad
July 2011	Joint India IMF Training Program on AML/CFT.	Jointly by RBI and IMF	Pune, India
April 2011	Joint EAG/ World bank Risk Assessment Workshop	EAG & World Bank	Kiev (Ukraine)
May 2011	Conference on financial flows linked to piracy off the coast of Somalia	UNODC	Nairobi, Kenya
May 2011	Training workshop on analytical methods and special technologies of conducting AML/CFT investigation.	International Training and Methodology Centre for Financial Monitoring (ITMCFM), EAG	Moscow
June 2011	Workshop on countering the financing of terrorism and anti -money laundering.	UNODC	Kabul (Afghanistan)
June 2011	Financial aspect of piracy	Republic of Korea	Seoul (South Korea)
August 2011	Analyst exchange programme between FIU-IND and FINCEN	FINCEN	Virginia (USA)
September 2011	Egmont Group/World Bank strategic analysis course	Egmont Group / World Bank	Doha (Qatar)
October 2011	Meeting on contact group of Somali piracy	UNODC	Rome (Italy)
December 2011	Joint FATF/ APG typologies workshop	FATF/APG	Busan (South Korea)

Chapter 8

Strengthening IT infrastructure

Project FINnet

FIU-IND initiated project FINnet in 2006 with the objective to "Adopt industry best practices and appropriate technology to collect, analyze and disseminate valuable financial information for combating money laundering and related crimes".

Objectives of the Project FINnet:

i) Build efficient system for collection of data from Reporting Entities to reduce the lead time in processing the data.

ii) Build capacity to effectively analyze large number of reports and produce quality intelligence.

iii) Build efficient system for dissemination and exchange of information with other Agencies.

iv) Build adequate internal capacity in terms of administrative support and knowledge base that will make FIU-IND an agile organization to meet its changing needs.

v) Adopt an array of security measures and internal controls.

Design and Implementation Phases

The Project consisted of two phases i.e. Design phase and Implementation phase. The Design phase commenced in March 2007 with the appointment of Ernst & Young Pvt. Ltd. (E&Y) as Consultants. During this Phase, the functional and technical specifications for Project FINnet were finalized in active consultation with FIU-IND and other stakeholders. The

consultants also prepared a detailed Request for Proposal (RFP) for selection of the System Integrator.

The implementation phase started with the signing of contract with Wipro Ltd as the System Integrator on 25th Feb 2010. The timeline for validation and acceptance of the complete solution is two years from the effective date of contract. During this phase the Consultant would provide project management services. The SI would provide enhanced support for 1 year from the date of the acceptance of the complete solution. The enhanced support would include Administration of Databases, Systems and Network, Facility Management Services, External Users Help Desk Services and Website maintenance. The SI is also required to provide Maintenance Support for the software and hardware for an additional 2 years.

Collection of Information

A typical report contains information about related accounts, transactions, individuals, legal entities, and addresses in a structured manner together with their relationships.

In FINnet, the earlier fixed-width, multiple data files reporting format has been replaced by a new single XML file format. The revised XML format supports effective data quality management, report life cycle management, compliance management, operational analysis, and strategic analysis. The details of reporting format specifications are given in the reporting format guide.

FIU-IND has provided report generation utility (RGU) to assist reporting entities in generation of the prescribed XML report from various data sources. The Report Validation Utility (RVU) enables users to validate an XML report before submission to FIU-IND.

The FINnet Gateway Portal is designed as a comprehensive interface between the reporting entities and FIU-IND to submit reports and exchange information. The portal enables users to upload reports and download data quality reports and additional request for information.

The portal also offers a comprehensive shared repository of resources like discussion forums, FAQs, problems and solutions and downloads. Messaging module and user groups enable collaboration of users within the portal.

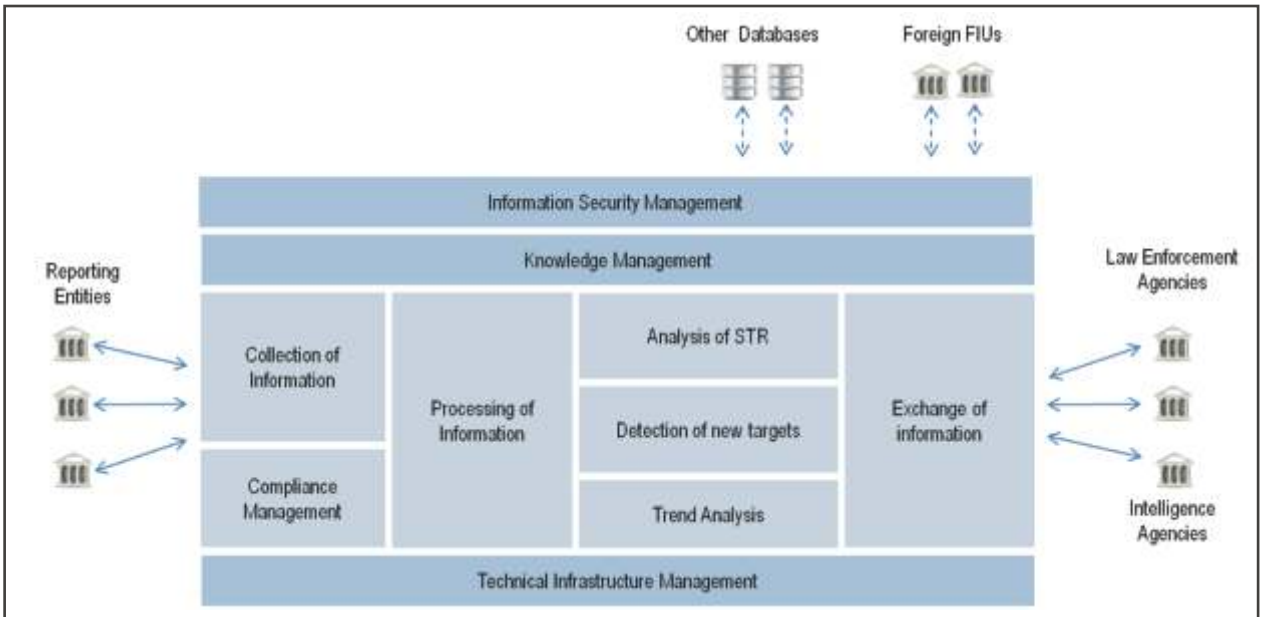


Figure: Schematic overview of FINnet

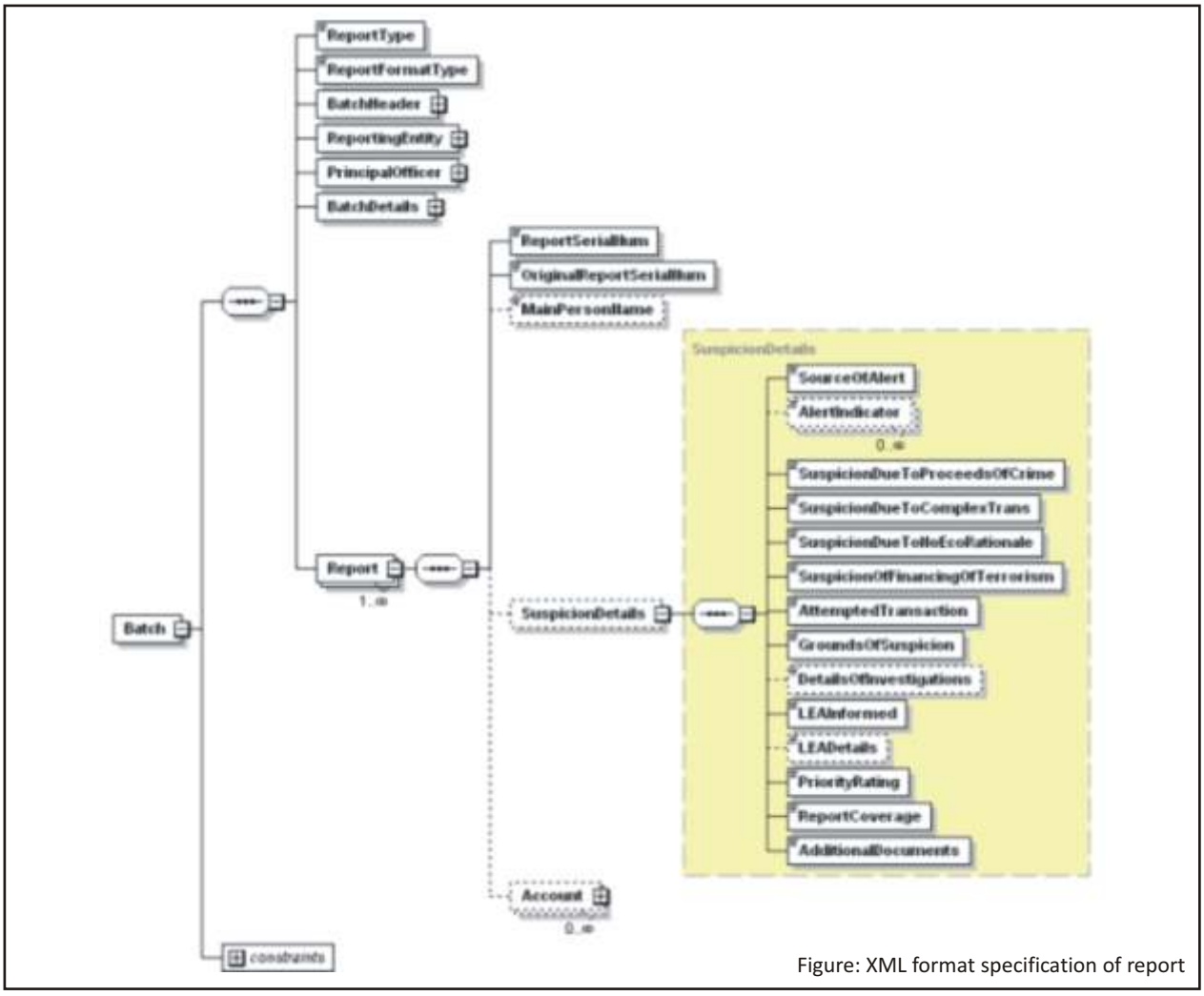


Figure: XML format specification of report

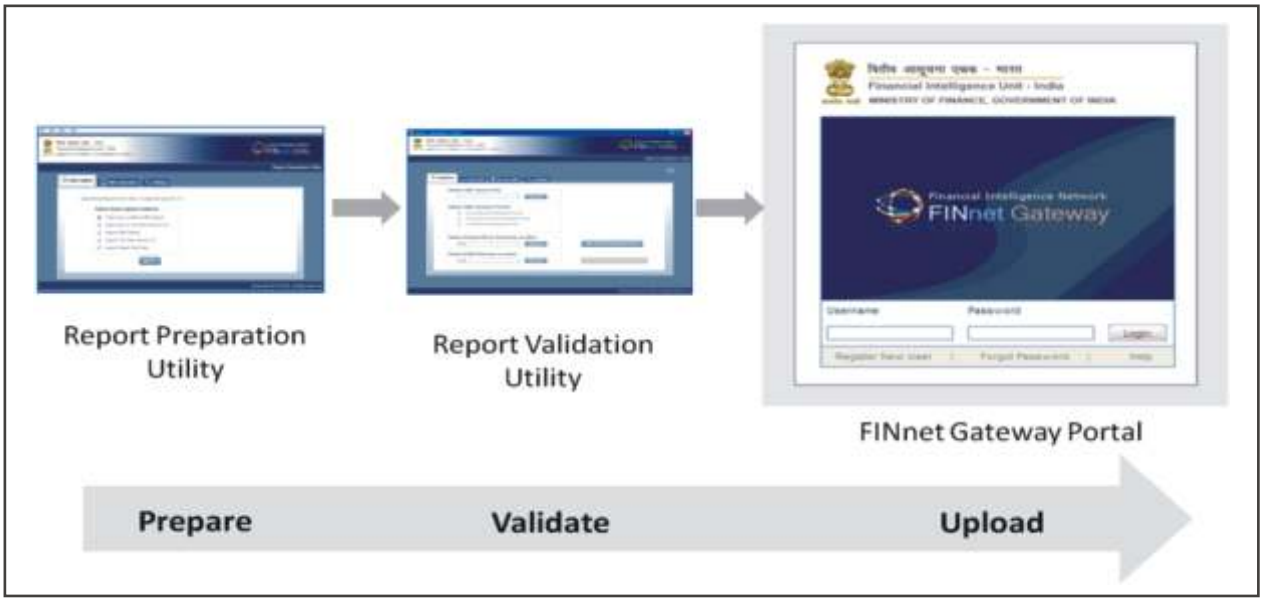


Figure: Steps in collection of information using FINnet Gateway portal

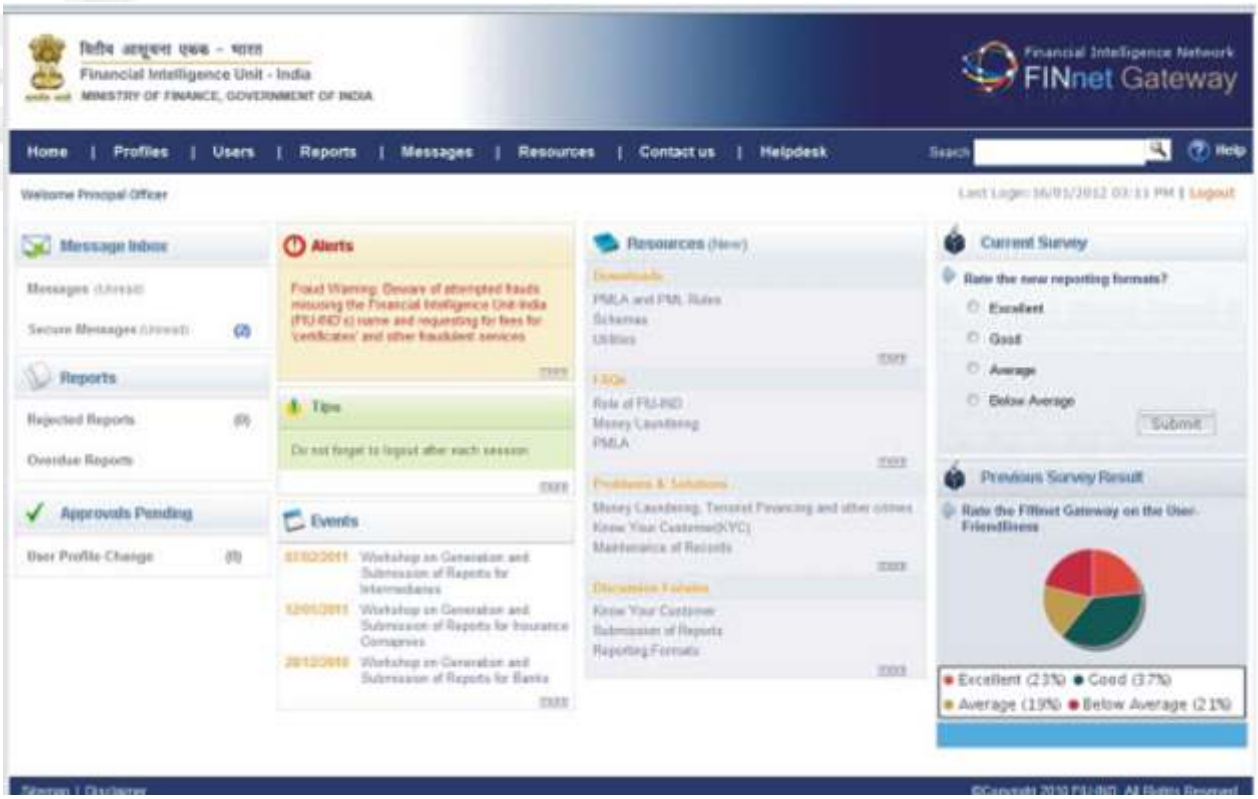


Figure: FINnet Gateway Portal for reporting entities

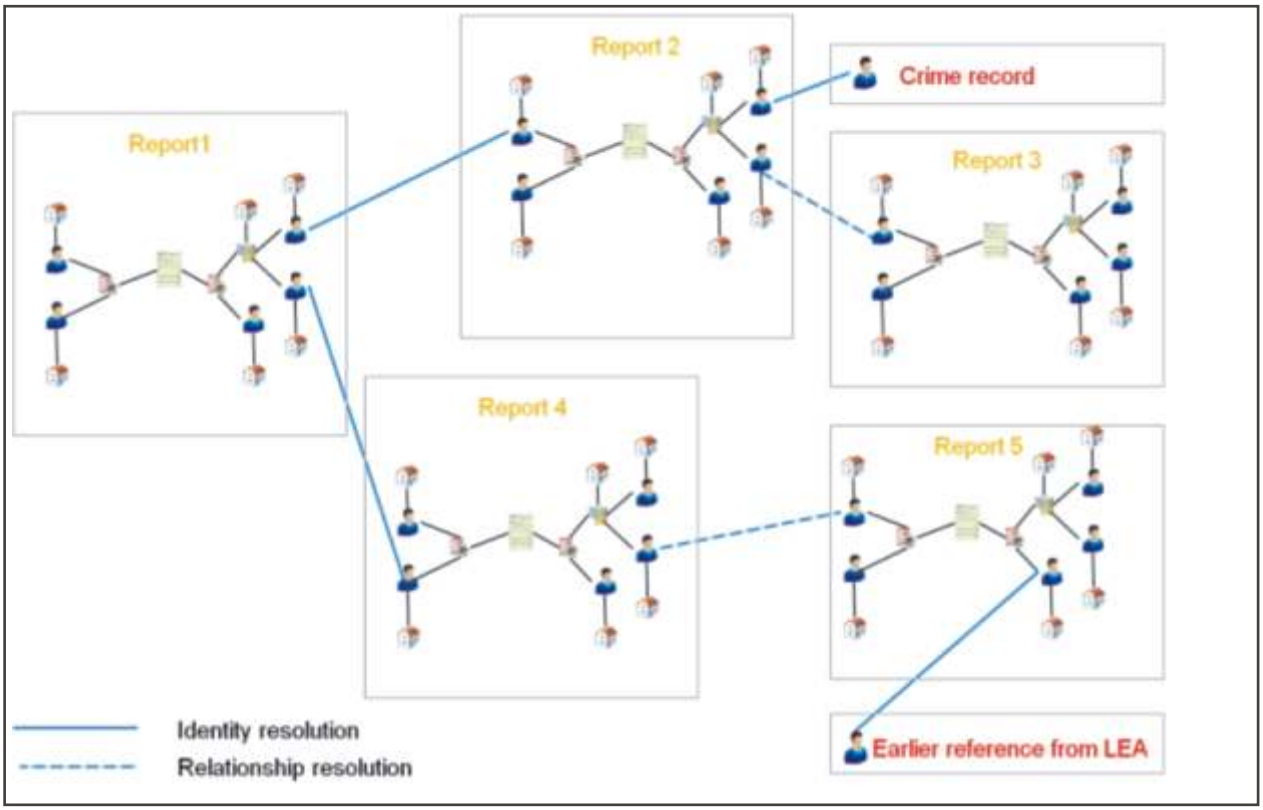


Figure: Clustering of report by identity and relationship resolution

STR Case Details

Case ID	1000001079	Priority	Normal	Analysis Type	Standard
ARMS Score	1	Initiation Date	01-10-2010	Expected End Date	15-10-2010

Case Summary

	In Primary STR	Linked by FIU	Total
STRs	1	2	3
CTRs	-	43	43
Individuals	1	1	2
Legal Entities	-	2	2
Accounts	3	5	8
Addresses	3	5	8
Debit Transactions (Number)	30	550	580
Credit Transactions (Number)	23	450	473
Debit Transactions (INR)	30,00,000	5,00,00,000	5,30,00,000
Credit Transactions (INR)	3,00,000	6,60,00,000	6,63,00,000

Related Individuals

XYZ	Address, Address	1	0 WL, 1 REQ, 2 STR, 31 CTR	R-
ABC	Address, Address	1	1 WL, 2 REQ, 2 STR, 43 CTR	R-I-R-

Related Legal Persons/Entities

Abc Ltd.	Address, Address	1	0 WL, 0 REQ, 2 STR, 37 CTR	R-I-R-L-R-
Xyz Pvt. Ltd.	Address, Address	1	0 WL, 0 REQ, 2 STR, 34 CTR	R-I-R-L-R-

Related Accounts

Figure: Review of STR case by Analyst at FIU

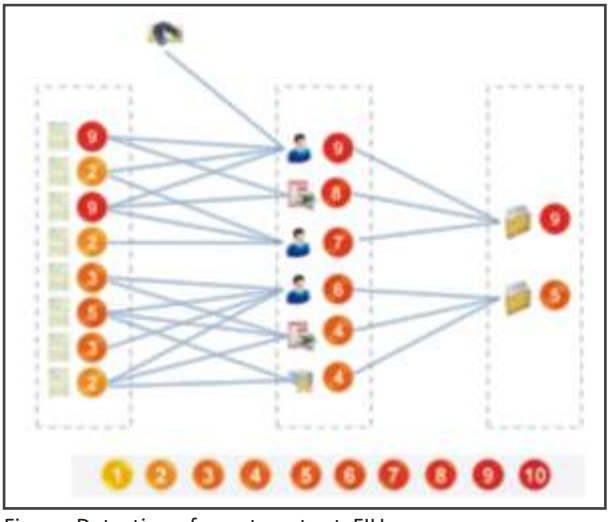


Figure: Detection of new targets at FIU

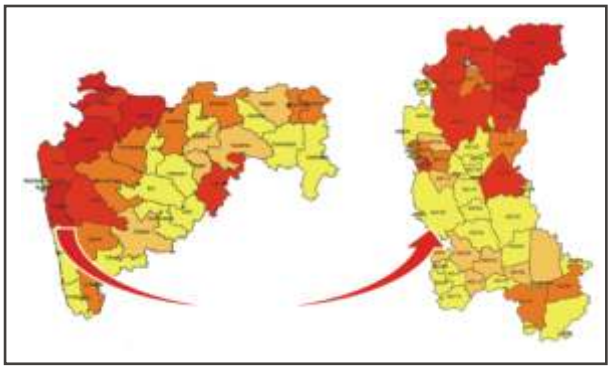


Figure: Geographical distribution with drill down

Processing of Information

The reports are first processed in a collection processing system which involves:

- Validation of reports using data validation rules and data sufficiency checks
- Generation of data quality report for the reporting entities
- Standardization of name and address fields
- Identification of linkages in the reports
- Resolution of unique identities and relationships in the report database

Reports related with 'n' degrees of separation are linked to form cases as per configurable rules. Key parameters of reports, persons, accounts and locations are summarized for efficient and effective analysis. Rule based engine is used for prioritization and allocation of cases.

Analysis of STR

STR analysis module of FINnet core presents the preprocessed dossier of the STR along with linkages with other related reports. Analyst can review system derived resolutions and linkages and make changes as required. Additional information can be requested from reporting entities or domestic agencies. Documents, charts and link diagrams can also be attached to the case.

A case decision making process is enabled, wherein analyst can decide to retain or disseminate a case. In case of dissemination, the analyst can select the agencies and users for dissemination. The system also enables a staggered dissemination. The cases are published in PDF and XML format.

Detection of New Targets

A comprehensive risk management system consisting of data mining tool and rule based engine is used to assess the risk in CTRs, STRs, persons, accounts, and cases using 82 pre-defined scenarios. The risk scores are computed and aggregated using a risk based approach.

The alert management system enables analysts to identify and filter high risk reports, persons, accounts, and cases using configurable thresholds. The system also enables geographical filtering at country, state, district and pin code levels.

The list management module helps the analyst in detecting new targets by applying complex scenarios.

Trend Analysis

Trend analysis is built on a business intelligence software to identify trends in reports, suspicion types, counterfeit currency incidents, remittances and card transactions.

Figure: Compliance related information of reporting entity

The trends can be analysed over time periods or geographies.

The trend analysis is integrated with digital maps to present geographical distribution of values or percentage change with drill down to the state, district and pincode level.

Compliance Management

The compliance management module of FINnet maintains comprehensive profile of reporting entities covering:

- Reporting Entity Information
  - Principal officer details
  - Report submission information
  - Data quality in reports
  - Training provided
  - Feedback provided
- Compliance related information
  - Compliance alerts
  - Preliminary compliance assessment
  - Compliance history assessment
  - Detailed compliance review
  - Compliance management

Figure: FINnet Exchange for domestic agencies

Exchange of information

FINnet Exchange (FINex) enables seamless exchange of information with domestic agencies. Spontaneous exchange of information includes a preview stage, in which a sanitized version of the case is shared with the users. On acceptance of spontaneous dissemination, all the details of the case become available as a downloadable PDF and XML. The FINex user can customize notifications alerts and networking alerts on the cases accessed by them.

FINex users can request for information from FIU through the portal. Bulk requests for information can also be uploaded as an XML file. FINex users are provided with a utility to generate bulk requests in XML format. FINex also provides web service to confirm existence of information in FIU databases. The requests are processed through the case analysis module in the FINnet Core and subsequently disseminated to the requesting person. The user can also provide feedback on the cases accessed by them.

The FINex portal also provides a messaging system and comprehensive shared repository of resources including discussion forums, FAQs, problems and solutions etc.

Knowledge Management

FINnet includes a comprehensive Knowledge Managements System (KMS) to support the following

- Library to manage upload, review and retrieval of documents
- Meeting place to manage team meetings
- Team Blog to display journal or diary
- Team Place to manage team content
- Team Wiki for creation and maintenance of content

Conclusion

FINnet substantially enhances the efficiency and effectiveness of FIU-IND's core function of collection, analysis and dissemination of financial information. IT enablement of key processes ensures higher productivity, faster turnaround time and effective monitoring in all areas of FIU-IND's work.

Function	Area of work	Current Situation	Outcome of Project FINnet
Collection	Preparation of electronic report by reporting entity	In- house developed Excel based utility to prepare electronic reports in fixed width text format	Advanced utilities to prepare, validate and encrypt electronic reports in XML format
	Receipt of electronic reports	Data is received on CD by post which takes 2-5 days	Online secure gateway to receive reports
	Data capture from manual reports	Data entry of only critical fields	Scanning and extraction of data
	Validation of Data Quality	Offline validation of data quality in batch mode	Streamlined process for Data Quality validation and feedback
	Communication with the Principal Officer	Through letters	Through a messaging system
Analysis	Verification of sufficiency of information	No check for sufficiency of information (incomplete name, address)	Checks for insufficient information fields using customized dictionaries
	Linkage of reports pertaining to same person	Basic de-duplication	Advanced de-duplication to overcome name and address variations
	Identification of relationships between persons	Identification of only explicit relationships	Identification of both explicit and implicit relationships
	Risk assessment and prioritization of cases	Manual decision making	Rules based systems to assign risk and prioritize alerts
	Search for additional information during analysis	Search using manual input by analyst	Automated advanced search and resolution before the case is made available to the analyst
	Access to external information sources	Manual input required	Streamlined exchange mechanism
	Generation of alert from Cash Transaction Reports (CTRs)	CTRs are used for adding value during processing of Suspicious Transaction Report (STR) or processing of references	Alerts will be generated from analysis of CTRs for further processing
	Identification of suspicious transaction patterns in reports	Manual interpretation	Automated detection of suspicious transaction patterns using data mining tools
	Analysis of trends in reports	Basic trend analysis using adhoc tools	Advanced trend analysis using Business Intelligence tools
Dissemination and Exchange	Spontaneous dissemination of information to domestic agencies	Through letters	Secure role based access
	Request based exchange with agencies	Through letters	Secure role based access using agreed information exchange protocol

The KMS provides following functionalities for effective knowledge management:

- Categorization of users as manager, editor, contributor or reader
- Support for serial and parallel approval process
- Support for document versioning
- Tagging of document to different categories
- Creating a view which can be shared
- Content search and advanced search

Technical Infrastructure Management

The technical infrastructure is hosted in the Primary Data Centre at New Delhi with a disaster recovery site at Hyderabad. An Enterprise Monitoring System (EMS) is deployed with dedicated internal and external helpdesk to enable:

- Network monitoring to discover and monitor devices in network infrastructure.
- Server management to manage the performance and availability of the servers
- Business service management to manage business applications and services
- Helpdesk to log the queries and incidents as tickets and manage the incidents and requests
- Generation of reports related to resource utilization, performance indicators and service levels

The system ensures single point accountability, multi-technology expertise, adherence to SLAs and business continuity.

Information Security Management

FINnet implements an array of security measures and internal controls to protect the information from unauthorized disclosure and provide reasonable assurance regarding prevention or prompt detection of unauthorized acquisition, use, or disposition of information assets.

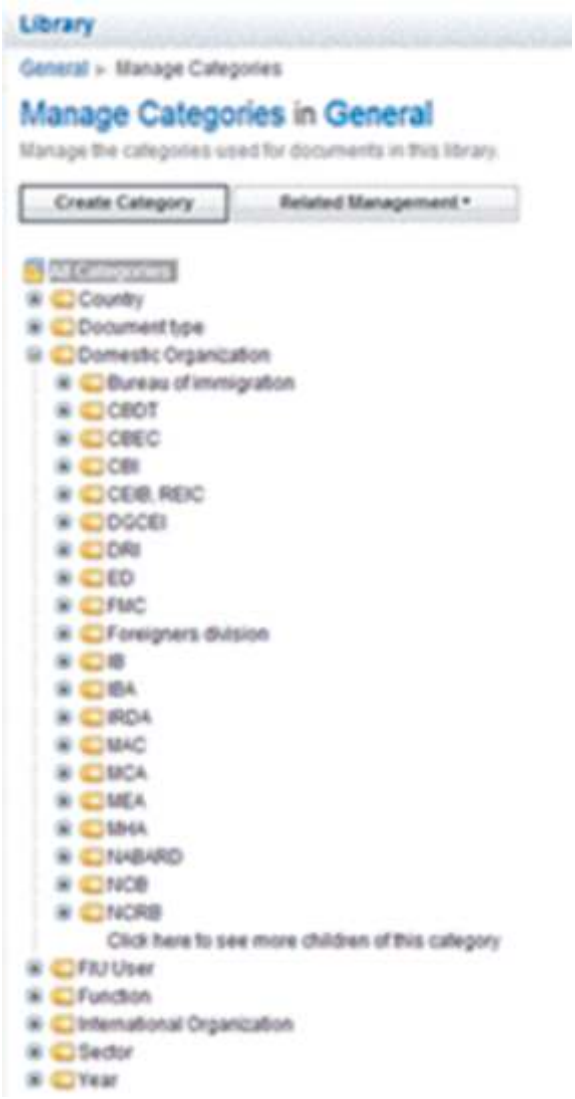


Figure: Category hierarchy in KMS

Figure: Enterprise monitoring system

Appendices

Appendix A - Staff strength of FIU-IND

Post	Sanctioned Strength	Working as on March 31, 2011
Director	1	1
Additional Director	10	7
Technical Director	1	1
Joint Director Systems (earlier Principal System Analyst)	1	0
Deputy Director Systems	2	1
Deputy / Assistant Director (earlier Senior Technical Officer)	21	9
Assistant Director Systems (earlier System Analyst/ Programmer)	6	0
Group B, C & D	33	12
Total	75	31*

* In addition 22 persons were working on contract basis

Appendix B - Chronology of Events for FIU-IND

2004-05	
Nov 18, 2004	Setting up of Financial intelligence unit- India (FIU-IND)
Mar 16, 2005	Appointment of First Director and FIU-IND becomes operational
2005-06	
Jul 1, 2005	PMLA and Rules thereunder brought into force
Mar 16, 2006	Launch of FIU-IND's website by the Hon'ble Finance Minister
2006-07	
Apr 3-5, 2006	On site visit of the Operational Working Group (OpWG) of the Egmont Group
Apr 13, 2006	Visit of the high level FATF delegation to FIU-IND
Jun 12-16, 2006	Attended Plenary session of the Egmont Group at Cyprus
Nov 6, 2006	Visit of high level delegation of the Counter Terrorism Executive Directorate (CTED) to FIU-IND
Feb 19-23 , 2007	Attended meeting of FATF Plenary at Strasbourg, France
Mar 29, 2007	Commencement of Project FINnet
2007-08	
May 16-17, 2007	Attended meeting of the Joint Working Group (JWG-CT) with Uzbekistan at Tashkent
May 28-Jun 1, 2007	Attended Egmont Plenary Session at Bermuda
May 29, 2007	FIU-IND becomes member of Egmont Group
May 29, 2007	Attended meeting of the Joint Working Group (JWG-CT) with UAE at Delhi
Jun 25-29, 2007	Attended FATF Plenary at Paris
Aug 28-31, 2007	Attended meeting of the Joint Working Group (JWG-CT) with Australia at Canberra
Oct 8-12, 2007	Attended FATF Plenary at Paris
Oct 16-18 , 2007	Attended Egmont Working Group Meeting at Kiev
Dec 7, 2007	Attended meeting of the Joint Working Group (JWG-CT) with Japan at Delhi
Feb 08, 2008	Attended meeting of the Joint Working Group (JWG-CT) with Canada at Delhi
Feb 11-12, 2008	Attended meeting of the Joint Working Group (JWG-CT) with Mauritius at Port Louis
Feb 11, 2008	Exchange of MoU with FIU of Mauritius
Feb 15, 2008	Visit of Sir James Sassoon, President FATF to FIU-IND
Feb 25-29, 2008	Attended FATF Plenary at Paris
Mar 11-13, 2008	Attended Egmont Working Group Meeting at Santiago, Chile
Mar 11, 2008	Signing of MoU with FIU of Philippines
2008-09	
May 25-29, 2008	Attended Egmont Plenary Session at Seoul
May 27, 2008	Signed MoU with Brazil
May 29, 2008	Visit of Mr. Antonio Gustavo Rodrigues, incoming FATF President to FIU-IND
Jun 16-20, 2008	Attended FATF Plenary at London
Aug 25, 2008	Joint Working Group (JWG-CT) meeting with USA at New Delhi
Oct 20-23, 2008	Attended Egmont Working Group Meeting at Toronto
Oct 21, 2008	Signed MoU with Malaysia
Dec 5, 2008	Signed Agreement with Russia
Dec 2, 2008	Joint Working Group (JWG-CT) meeting with UK at New Delhi
Dec 16-17, 2008	Joint Working Group (JWG-CT) meeting with Russia at New Delhi
Feb 23-27, 2009	Attended FATF Plenary at Paris
Mar 2-5, 2009	Attended Egmont Working Group Meeting at Guatemala

Appendix B - (continued)

2009-10	
May 25-29, 2009	Attended 17th Egmont Plenary Session at Doha, Qatar
May 26, 2009	Signed MoU with AUSTRAC, Australia
Jun 11, 2009	Joint Working Group (JWG-CT) meeting with EU at New Delhi
Oct 12-16,2009	Attended FATF Plenary Session at Paris, France
Oct 19-22,2009	Attended Egmont Working Group Session at Kuala Lampur, Malaysia
Oct 21, 2009	Signed MoU with Canada
Nov 20, 2009	Signed MoU with Directorate of Enforcement
Dec 1, 2009	Visit of FATF/ APG Mutual Evaluation Team to FIU-IND
Feb 15-19, 2010	Attended FATF Plenary Session at Abu Dhabi
Feb 25, 2010	Signed contract with M/s Wipro Ltd. for execution of Project FINnet
Feb 25, 2010	JAFIC delegation visits FIU-IND
Feb 28-Mar 4, 2010	Attended Egmont Working Group Session at Port Louis, Mauritius
Mar 3, 2010	Signed MoU with FINCEN, USA
Mar 26, 2010	Signed MoU with FIU of Sri Lanka
2010-11	
Apr 26-30,2010	Meeting with FATF Assessment Team at Sydney, Australia
May 5, 2010	Signed MoU with FIU of Georgia
June 10, 2010	Signed MoU with Financial Intelligence Agency, San Marino
June 20-25, 2010	Attended FATF Plenary meeting at Amsterdam, Netherlands
June 25,2010	India becomes member of FATF
June 27- July 1,2010	Attended 18th Egmont Group Plenary at Cartagena, Columbia
July 1,2010	India becomes Co-chair of Asia Group in Egmont Committee
July12- 16, 2010	Attended APG Annual Meeting at Singapore
Oct. 4 -7, 2010	Participated in Tactical Analysis Course at Kuala Lumpur, Malaysia
Oct. 11 - 13, 2010	Attended Egmont Working Group and Committee Meetings at Chisinau, Moldova
Oct. 12, 2010	Signed MoU with Financial Intelligence Agency, Bermuda
Oct. 12, 2010	Signed MoU with Nigerian Financial Intelligence Unit, Nigeria
Oct. 18 - 22, 2010	Attended FATF Plenary at Paris, France
Oct. 25-28, 2010	Attended 2010 APG Typologies Workshop at Dhaka, Bangladesh
Nov. 8, 2001	Signed MoU with Japan Financial Intelligence Centre, Japan
Nov. 15-19, 2010	Attended FATF/Egmont Group Joint Experts Meeting on ML/TF Typologies at Cape Town, South Africa
Dec. 6-10, 2010	Attended Regional Advanced Analysis Skills workshop at Kuala Lumpur
Dec. 15, 2010	India becomes member of EAG
Jan. 25, 2011	Signed MoU with FINTRAC/PPATK, Indonesia
Feb. 21-25, 2011	Attended FATF Plenary at Paris, France
March 1, 2011	Attended ad-Hoc meeting on Financial Aspects of Piracy off the coast of Somalia at Washington, USA
Mar. 14-17, 2011	Attended Egmont Working Group (EWG) and Committee Meetings at Oranjestad, Aruba
Mar. 31, 2011	Phase I of Project FINnet completed

Appendix B - (continued)

2011-12	
Apr 05-07, 2011	Attended regional workshop organized by AUSTRAC at Kathmandu, Nepal
Apr 21-22, 2011	Attended workshop organized by World Bank & EAG at Kiev, Ukraine
May 9-14, 2011	Attended training program on Prevention of Insurance Frauds at NIA, Pune
June 6-10, 2011	Attended training program organized by IMF at NIBM, Pune
June 14-17, 2011	Attended EAG Plenary & Working Group Meetings at Moscow, Russia
June 29, 2011	Attended 2nd Ad-hoc Meeting of Financial Aspect of Piracy at Seoul, South Korea
July 11-15, 2011	Attended training program organized by IMF at NIBM, Pune
July 11-15, 2011	Attended 19th Egmont Group Plenary at Yerevan, Armenia
July 12, 2011	Signed MoUs with FIUs of Israel and Poland
Aug. 22-25, 2011	Attended Analyst Exchange Program organized by FinCEN (US FIU) at Virginia, USA
Sept. 12-15, 2011	Attended Strategic Analysis Course organized by FIU, Qatar
Sept. 22-24, 2011	An officer visited FIU Mauritius to provide technical assistance and assessing their IT Infrastructure
Sept. 26-30, 2011	Attended FATF meeting at Rome, Italy
Oct. 7, 2011	Attended First Meeting of Working Group-5 of the Contact Group on Somali Piracy at Italy
Oct. 21-28, 2011	Attended FATF plenary at Paris
Oct. 24, 2011	Signed MoU with FIU, Singapore
Nov. 2-7, 2011	A team visited FIU Bhutan to provide technical assistance for setting up FIU
Nov. 23-25, 2011	Attended 15th EAG plenary at Xiamen, China
Nov. 17, 2011	Signed MoU with Nepal
Dec. 9, 2011	Attended Joint APG/ Egmont Group FIU seminar at Busan, Korea
Jan. 30- Feb. 3, 2012	Attended EWG meetings at Manila, Philippines
Feb. 13-17,2012	Attended FATF Plenary and Working Group Meetings at Paris, France
Mar. 19-20, 2012	Attended 4th meeting of BIMSTEC at Bangkok, Thailand
Mar. 26, 2012	Phase II of Project FINnet completed

Appendix C- Predicate offences under PMLA

PMLA (Amendment) Act, 2009 expanded the list of schedule offences under PMLA. The expanded list (effective from 1st June 2009) is as under:

Part A of the Schedule: Offences under:

- The Indian Penal Code,1860 (S.121 & 121A, S.489A & 489B)
- The Narcotic Drugs & Psychotropic Substances Act, 1985 (S.15,16,17,18,19,20,21,22,23,24,25A, 27A & 29)
- The Explosive Substances Act, 1908 (s.3, 4 & 5)
- The Unlawful Activities (Prevention) Act, 1967 (S.10 read with S.3, S.11 read with S.3 & 7, S.13 read with S.3, S.16 read with S.15, S.16A,17,18,18A, 18B, 19, 20, 21, 38, 39 &40)

Part B of the Schedule: Offences under:

- The Arms Act, 1959 (S.25,26,27,28,29 & 30)
- The Explosives Act, 1884 (S.9B & 9C)
- The Wildlife (Protection) Act, 1972 (S.51 read with S.9, S.51 read with 17A, S.51 read with 39, S.51 read with 44, S.51 read with 48 & S.51 read with 49B)
- The Immoral Traffic (Prevention) Act, 1956 (S.5,6,8 & 9)
- The Prevention of Corruption Act, 1988 (S.7,8,9,10 & 13)
- The Indian Penal Code (S.120B,255,257,258,259,260,302,304,307,308,327,329,364A,384 to 389,392 to 402,411, 412,413,414,417,418,419,420,421,422,423,424,467,471,472,473,475,476,481,482,483,484,485,486,487 & 488)
- The Antiquities and Art Treasures Act, 1972 (S.25 read with S.3, S.28)
- The SEBI Act, 1992 (S.12A read with S.24)
- The Customs Act, 1962 (S.135)
- The Bonded Labour System (Abolition) Act, 1976 (S.16,18 & 20)
- The Child Labour (Prohibition and Regulation) Act, 1986 (S.14)
- The Transplantation of Human Organs Act, 1994 (S.18,19 & 20)
- The Juvenile Justice (Care and Protection of Children) Act, 2000 (S.23,24,25 & 26)
- The Emigration Act, 1983 (S.24)
- The Passports Act, 1967 (S.12)
- The Foreigners Act, 1946 (S.14,14B & 14C)
- The Copyright Act, 1957 (S.63,63A,63B & 68)
- The Trade Marks Act, 1999 (S.103,104,105,107 & 120)
- The Information Technology Act, 2000 (S.72 & 75)
- The Biological Diversity Act, 2002 (S.55 read with S.6)
- The Protection of Plant Varieties and Farmer's Rights Act, 2001 (S.70 read with S.68, S.71 read with S.68, S.72 read with S.68 & S.73 read with S.68)
- The Environment Protection Act, 1986 (S.15 read with S.7 & S.15 read with S.8)
- The Water (Prevention and Control of Pollution) Act, 1974 (S.41(2) & 43)
- The Air (Prevention and Control of Pollution) Act, 1981 (S.37)
- The Suppression of Unlawful Acts against Safety of Maritime Navigation and Fixed Platforms on Continental Shelf Act, 2002 (S.3)

Part C of the Schedule**:**

- Cross border offences without any monetary threshold covering all offences specified in Part-A, or Part-B without any threshold, or offences against property under chapter XVII of the Indian Penal Code.

Appendix D - Important Rules/Notifications

Date	Not. No.	Description
01.07.2005	1/2005	Appointed 1st July 2005 as the date on which all the provisions of the Prevention of Money Laundering Act, 2002 shall come into force.
01.07.2005	2/2005	Appointed an Adjudicating Authority to exercise jurisdiction, powers and authority conferred by or under the Prevention of Money Laundering Act, 2002. The Adjudicating Authority shall consist of a Chairperson and two members and shall function within the Department of Revenue, Ministry of Finance of the Central Government with Headquarters at Delhi .
01.07.2005	3/2005	Specified that the New Delhi Bench of the Adjudicating Authority shall exercise jurisdiction, powers and authority conferred by or under the Prevention of Money Laundering Act, 2002 over the whole of India .
01.07.2005	4/2005	Established an Appellate Tribunal at New Delhi to hear appeals against the orders of the Adjudicating Authority and the authorities under the Prevention of Money Laundering Act, 2002.
01.07.2005	5/2005	Conferred certain exclusive and concurrent powers under the Prevention of Money Laundering Act, 2002 to the Director, Financial Intelligence Unit, India .
01.07.2005	6/2005	Conferred certain exclusive and concurrent powers under the Prevention of Money Laundering Act, 2002 to the Director of Enforcement.
01.07.2005	7/2005	Specified Rules relating to the manner of forwarding a copy of the order of provisional attachment of property along with the material, and the copy of the reasons along with the material in respect of survey, to the Adjudicating Authority and its period of retention by the Adjudicating Authority.
01.07.2005	8/2005	Specified Rules for receipt and management of confiscated properties.
01.07.2005	9/2005	Specified Rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients of the banking companies, financial institutions and intermediaries of securities market.
01.07.2005	10/2005	Specified Rules relating to the Forms, search and seizure and the manner of forwarding a copy of the reasons and the material relating to search and seizure and search of person to the Adjudicating Authority, impounding and custody of records and the period of retention thereof.
01.07.2005	11/2005	Specified Rules relating to the Forms, the manner of forwarding a copy of the order of arrest of a person along with the material to the Adjudicating Authority and the period of retention there of by the Adjudicating Authority.
01.07.2005	12/2005	Specified Rules relating to the manner of forwarding a copy of the order of retention of seized property along with the material to the Adjudicating Authority and its period of retention by the Adjudicating Authority.
01.07.2005	13/2005	Specified Rules for the manner of receiving the records authenticated outside India.
01.07.2005	14/2005	Specified Rules for the purpose of appeals under the Prevention of Money Laundering Act, 2002.
13.12.2005	15/2005	Amended Rules 5, 7, 8 and 10 of the Rules notified by Notification No. 9/2005
27.06.2006	6/2006	Specified the authorities to whom Director, FIU-IND can furnish information under Section 66 of the PMLA
24.05.2007	4/2007	Amended definition of suspicious transaction (Rule 2), counterfeit currency transaction (Rule 3(1)(C)), due dates for furnishing reports (Rule 8) and requirement of verification of the records of the identity of clients (Rule 9)
12.11.2009	13/2009	Amended Rule 2, 3, 5, 6,7, 8, 9 and 10 of the Rules notified by Notification No. 9/2005.
12.02.2010	67/2010	Amended requirements of maintenance of accounts and definition of beneficial owner.
16.06.2010	10/2010	Amended rule 2, 9 & 10 to include explanation to the definition of 'suspicious transaction' on transactions involving financing of activities related to terrorism, obligation to determine beneficial owner, ongoing due diligence, prohibition on keeping or opening anonymous or fictitious accounts, etc.
16.12.2010	14/2010	Amended rule 2 and 9 to expand the list of 'officially valid documents' (Rule 2) by including letter issued by NREGA and Aadhar number issued by UIDAI and inserted provisions to enable opening of 'small account'.
24.06.2011	6/2011	Amended the name of PMLA rule as notified vide Notification No 9/2005 to 'The Prevention of Money Laundering (Maintenance of Records) Rules, 2005'.

Appendix E - Important Circulars & Instructions issued by the Regulators

Reserve Bank of India	
29.11.2004	KYC Guidelines-AML Standards- Scheduled Commercial banks
15.12.2004	KYC Guidelines-AML Standards- Primary Urban Co-operative Banks
18.02.2005	KYC Guidelines-AML Standards- State Co-operative Banks and District Central Co-operative Banks
18.02.2005	KYC Guidelines-AML Standards - Regional Rural Banks
23.08.2005	KYC Guidelines-AML Standards - Scheduled Commercial Banks
23.08.2005	KYC Guidelines-AML Standards- Primary Urban Co-operative Banks
23.08.2005	KYC Guidelines-AML Standards - State Co-operative Banks and District Central Co-operative Banks
23.08.2005	KYC Guidelines-AML Standards - Regional Rural Banks
11.10.2005	KYC for persons authorised by NBFCs including brokers/agents etc. to collect public deposit on behalf of NBFCs
21.11.2005	Credit card operations of banks- Scheduled Commercial Banks/NBFCs
2.12.2005	Anti-Money Laundering Guidelines for Authorised Money Changers
15.02.2006	PMLA- Obligation of banks in terms of Rules notified thereunder - Scheduled Commercial Banks
3.03.2006	PMLA- Obligation of banks in terms of Rules notified thereunder - State Co-operative Banks and District Central Co-operative Banks
7.03.2006	KYC Guidelines-AML Standards-NBFCs, Miscellaneous Non-Banking Companies, Residuary Non-Banking Companies
9.03.2006	PMLA- Obligation of banks in terms of Rules notified thereunder - Regional Rural Banks
21.03.2006	PMLA- Obligation of banks in terms of Rules notified thereunder - Primary Urban Co-operative Banks
05.04.2006	PMLA- Obligation of NBFCs in terms of Rules notified thereunder - NBFCs, Miscellaneous Non-Banking Companies, Residuary Non-Banking Companies
26.06.2006	Anti-Money Laundering Guidelines for all authorsied persons in Foreign Exchange
16.11.2006	Compliance function of Banks- Scheduled Commercial Banks
17.04.2007	Circular on Safe Deposit Lockers includes Customer Due Diligence for allotment of lockers
13.04.2007	KYC Norms/AML Standards/CFT - Wire Transfers - Scheduled Commercial Banks
20.04.2007	Compliance function of Banks- Scheduled Commercial Banks
18.05.2007	KYC Norms/AML Standards/CFT - Wire Transfers - State Co-operative Banks and District Central Co-operative Banks
21.05.2007	KYC Norms/AML Standards/CFT - Wire Transfers -Regional Rural Banks (RRBs)
25.05.2007	KYC Norms/AML Standards/CFT - Wire Transfers -Primary Urban Co-operative Banks
17.10.2007	Anti-Money Laundering Guidelines for all authorsied persons in Foreign Exchange
18.02.2008	KYC Norms/AML Standards/CFT - Scheduled Commercial Banks
25.02.2008	KYC Norms/AML Standards/CFT- Primary Urban Co-operative Banks
27.02.2008	KYC Norms/AML Standards/CFT-Regional Rural Banks
28.02.2008	KYC Norms/AML Standards/CFT- State Co-operative Banks and District Central Co-operative Banks
22.05.2008	Circular on KYC norms/AML/CFT obligation of banks
01.07.2008	Master Circular on KYC norms/AML/CFT obligation of banks
23.06.2009	List of Terrorist Individuals/Organisations - under UNSCR 1267(1999) and 1822(2008)
01.07.2009	Master Circular - KYC norms / AML standards/ CFT/Obligation for Scheduled Commercial Banks
01.07.2009	Master Circular - KYC Guidelines - AML Standards for all NBFCs, MNBs, RNBs
01.07.2009	Master Circular - Para-banking Activities for all scheduled commercial banks (excluding RRBs)
01.07.2009	Master Circular - Foreign Contribution (Regulation) Act, 1976
01.07.2009	Master Circular - KYC Guidelines - AML Standards for all NBFCs, MNBs, RNBs
19.11.2009	KYC norms/ AML standards/CFT - Obligation of Authorised Persons - Money changing activities
11.08.2009	List of Terrorist Individuals/Organisations - under UNSCR 1267(1999) and 1822(2008)
14.08.2009	Use of RTGS/NEFT/NECS/ECS - Compliance with FEMA Regulations and Wire Transfer Guidelines

Appendix E (continued)

14.08.2009	Policy Guidelines for issuance and operation of Prepaid Payment Instruments in India
27.11.2009	KYC norms/ AML standards/CFT - Cross Border Inward Remittance under MTSS
11.09.2009	KYC norms / AML standards/CFT/Obligation of scheduled commercial banks
16.09.2009	Adherence to KYC/AML guidelines-Multi Level Marketing firms - Primary (Urban) Co-operative Banks
17.09.2009	CFT - Unlawful Activities (Prevention) Act, 1967 - Obligation of scheduled commercial banks
29.09.2009	KYC Norms / AML Standards and obligation of Regional Rural Banks (RRBs)
30.09.2009	KYC / AML Standards / CFT / Obligation of State and Central Co-operative Banks
29.10.2009	CFT- Unlawful Activities (Prevention) Act, 1967 - Obligation of State and Central Co-operative Banks
05.11.2009	CFT- Unlawful Activities (Prevention) Act, 1967 - Obligation of RRBs
13.11.2009	Prevention of Money Laundering Act, 2002 - Obligation of Urban Co-operative Banks (UCBs)
13.11.2009	KYC Norms/AML Standards/CFT-Obligations under PMLA 2002 - NBFCs
16.11.2009	CFT- Unlawful Activities (Prevention) Act, 1967 - Obligation of UCBs
16.11.2009	KYC Norms/AML Standards/CFT-Obligations under PMLA 2002 - UCBs
27.11.2009	KYC norms/ AML standards/CFT - Obligation of Authorised Persons - Money changing activities
22.12.2009	KYC norms/ AML standards/CFT - Obligation of Payment System Operators
12.01.2010	Prevention of Money-laundering Amendment Rules, 2009 - Obligation of banks/Financial Institutions
26.03.2010	KYC guidelines - accounts of proprietary concerns - Obligation of Scheduled Commercial Banks
26.03.2010	KYC norms/AML Standards/CFT -Obligation of Scheduled Commercial Banks
01.07.2010	KYC norms/AML Standards/CFT -Obligation of Scheduled Commercial Banks
Apr - May, 2011	Anti-Money Laundering (AML) /Combating of Financing Terrorism (CFT) Standards. FATF Statement identifying a list of jurisdictions which have strategic AML/CFT deficiencies to Authorized Persons, MTSS, PSO, DCCBs,StCBs, Money Changing Activities, UCBs, NBFCs, RNBCs.
05.04. 2011	Operation of deposit accounts with NBFCs and money mules.
01.07.2011	Master Circular on Money Transfer Service Scheme.
01.07.2011	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, 2002. to All Scheduled Commercial Banks (Excluding RRBs)/ All India Financial Institutions/ Local Area Banks. UCBs
01.07.2011	Master Circular - KYC Guidelines - Anti-Money Laundering Standards - PMLA, 2002 - Obligations of NBFCs.
08.08.2011	Opening of "Small Account"
02.10.2011	Appointment of Agents/ Franchisees by Authorized Dealer Category - I banks, Authorized Dealer Category - II and Full Fledged Money Changers - Revised guidelines.
09.11.2011	UCBs - KYC Norms - Letter issued by UDAI containing details of name, address and Aadhaar number.
22.12.2011	KYC Norms/ AML Standards/CFT - Obligation of Authorized Persons under PMLA, 2002
30.12.2011	KYC Norms /AML Standards/CFT/Obligation of Banks under PMLA 2002 - Assessment and Monitoring of Risk.
Securities Exchange Board of India (SEBI)	
18.01.2006	Guidelines for Anti Money Laundering Measures
20.03.2006	Obligations of Intermediaries under the PMLA
27.04.2007	Permanent Account Number (PAN) to be the sole identification number
19.12.2008	Master Circular on AML/CFT -Obligations of Securities Market Intermediaries
01.09.2009	AML Standards/CFT-Obligations of Securities Market Intermediaries
23.10.2009	CFT under Unlawful Activities (Prevention) Act, 1967 - all registered intermediaries
14.06.2010	AML Standards / CFT -Obligation of Securities Market Intermediaries
05.10.2011	Uniform Know Your Client (KYC) requirements for the securities market.
25.10.2011	In-person verification (IPV) of clients by subsidiaries of Stock Exchanges, acting as Stock Brokers
02.12.2011	The Securities and Exchange Board of India (KYC Registration Agency) Regulations, 2011
23.12.2011	Guidelines in pursuance of the SEBI KYC Registration Agency (KRA) Regulations, 2011 and In-Person Verification (IPV)

Insurance Regulatory and Development Authority (IRDA)	
31.03.2006	Guidelines of Anti Money Laundering Programme for Insurers
24.11.2008	Master Circular on AML/CFT -Obligations of Insurance Companies
18.08.2009	Requirement of PAN for Insurance Products for Insurers
24.08.2009	AML Guidelines for Insurance Companies
13.05.2010	Prevention of Money-laundering Amendment Rules, 2010- Obligation of Insurers
16.06.2010	Anti Money Laundering Guidelines - Obligation of Insurers
28.10.2009	Guidelines for implementation of Section 51A of Unlawful Activities (Prevention) Amendment Act
09.09.2009	The Prevention of Money Laundering (Amendment) Act, 2009 for Insurance Companies
05.07.2011	Amendment to Rule 2(d) of PML (Maintenance of Records) Rules, 2005
05.10.2011	AML/CFT Guidelines - Cash Acceptance Threshold
01.01.2012	Amendment of clause 3.1.1(xiv) of the Master Circular 2010 on AML/CFT guidelines on conducting detailed due diligence while taking insurance risk exposure to individuals/ entities connected with countries identified by FATF as having deficiencies in their AML/CFT regime.
National Housing Bank (NHB)	
31.03.2005	KYC Guidelines - Identification of customers- for Housing Finance Companies
10.04.2006	KYC Guidelines / AML Standards for Housing Finance Companies
17.01.2007	KYC Guidelines / AML Standards -Reporting System for Housing Finance Companies
25.07.2007	KYC Guidelines / AML Standards -Reporting System for Housing Finance Companies
20.02.2009	KYC Norms/AML Standards / Combating of Financing of Terrorism (CFT) for Housing Finance Companies
23.06.2009	KYC Norms/AML Standards / Combating of Financing of Terrorism (CFT) for Housing Finance Companies
25.01. 2010	`Know Your Customer (KYC) Norms/ Anti-Money Laundering (AML) Standards/ Combating of Financing of Terrorism (CFT)
06.05.2011	Guidelines on "Know Your Customer"& Anti-Money Laundering Measures" for HFCs

Appendix F - Obligations of Reporting Entities under PMLA

Obligation	When
Communicate the name, designation and address of the Principal Officer to FIU-IND	At the time of appointment/ change of Principal Officer
Formulate and implement a Client Identification Programme (CIP) to determine true identity of clients	Initially and in pursuance of any change being prescribed by the Regulator
Identify the client, verify their identity and obtain information on the purpose and intended nature of the relationship	At the time of commencement of account-based relationship
Verify the identity of the client	At the time of carrying out a transaction for an amount equal to or exceeding Rupees fifty thousand or any international money transfer operation
Identify beneficial owner and a person acting on behalf of a client, where the client is a juridical person	At the time of commencement of the relationship and at the time of any change in beneficiary/ authorized person
Obtain a certified copy of documents in evidence of identity and address and a recent photograph and other documents in respect of the nature of business and financial status of the client (as may be prescribed by the Regulator)	At the time of commencement of account-based relationship
Evolve internal mechanism for maintaining and furnishing information	Ongoing
Maintain record of all transactions that allows reconstruction of individual transactions including the nature of transaction, the amount and currency of transaction, the date of the transaction and the parties of the transaction	Ongoing
Examine transactions and to ensure that they are consistent with the business and risk profile of the customer	As an ongoing due diligence
Furnish Cash Transaction Report (CTR) to FIU-IND containing specified cash transactions	Within 15th day of succeeding month (Monthly Reporting)
Furnish Counterfeit Currency Report (CCR) to FIU-IND Furnish report in respect of Non-Profit-Organizations (NPOs)	Within 7 working days from the date of transaction
Furnish Suspicious Transaction Report (STR) to FIU-IND all suspicious transactions whether or not made in cash, including attempted suspicious transaction	Within 7 working days on being satisfied that the transaction is suspicious
Maintain records of identity of clients	For a period of 10 years from the date of cessation of the transaction. The expression 'cessation of the transaction' means termination of an account or business relationship.
Maintain records of all transactions	For a period of 10 years from the date of transaction.

Appendix G - Interaction with Partner Agencies

May-11	Gujarat State Police Academy	Modalities of sharing information about crimes and criminals
	Gujarat State Police Academy	Training on Economic intelligence for senior Gujarat Police Officers
	National Academy of Customs, Excise and Narcotics, Faridabad	Role of FIU in implementation of PMLA, 2002
	CBI Academy, Ghaziabad	Financial Intelligence and role of FIU in detecting economic crimes
June-11	CBI Academy, Ghaziabad	AML Workshop on 'Financial Intelligence & Role of FIU' in detecting Economic Crime during Orientation Course for new officers joining CBI on deputation
	CBI Academy, Ghaziabad	Lecture on Money Laundering
	• National Academy of Customs, Excise and Narcotics, Mumbai	Lecture on "Prevention of Money Laundering & Role of Financial Intelligence Unit-India" during course on "Capacity Building on Economic Intelligence"
	• IMF Pune	Establishing an FIU: The Indian Experience
July-11	• National Academy of Customs, Excise and Narcotics, Mumbai	Lecture on "Prevention of Money Laundering & Role of Financial Intelligence Unit-India
	• National Academy of Customs, Excise and Narcotics, Mumbai	Lecture on "Prevention of Money Laundering & Role of Financial Intelligence Unit-India" during course on "Capacity Building on Economic Intelligence"
	• National Housing Bank, Ooty, Tamil Nadu	Prevention of Money Laundering and role of FIU-IND
	• LTU, New Delhi	Role of Financial Intelligence Unit-India in Prevention of Money Laundering
	• National Academy of Customs, Excise and Narcotics, New Delhi	Role of Financial Intelligence Unit-India in Prevention of Money Laundering
	• FIU-IND, New Delhi	Tracking the money trail to counter transnational organised crime
Aug-11	• Lal Bahadur Shastri National Academy of Administration, Mussoorie	"Role of FIU-IND in Combating Money Laundering and Financing of Terrorism".
	• National Police Academy, Hyderabad	General Overview of AML/CFT Regime & Role of FIU-IND
	• FIU-IND, New Delhi	Workshop on FIN net Exchange
	• CBI Academy, Ghaziabad	Lecture on 'Financial Intelligence & Role of FIU in detecting Economic Crime' during Orientation Course for new officers joining CBI on deputation
	• CBI Academy, Ghaziabad	Lecture on 'An Introduction to the Collection of Criminal Intelligence in economic offences with an Overview of FIU and its role in detection of economic offences" during course on "Investigation of Economic. Offences"

Oct-11	• NACEN, Mumbai	Course on PMLA
	• CBI, New Delhi	FIU-IND's Role in Anti-Corruption Drive
	• NACEN, New Delhi	Comparative Study of EP schemes & overview of AML framework
Nov-11	• Maharashtra Police Academy, Nashik	AML / CFT Regime & Police Officers
	• Mumbai Police, Mumbai	Intelligence sharing and need of Data bank for tracking offenders of Economic Crimes
	• NIA, New Delhi	Secure Exchange of Information
	• National Academy of Direct Taxes, Nagpur	Use of Information Technology Management, Information/Data Security, Data Mining
	• National Academy of Customs, Excise & Narcotics, Kanpur	Role of FIU for effective implementation of AML & CFT provisions
Jan-12	• FIU-IND, New Delhi	FINnet Exchange
	• National Savings Institute MOF, DEA, Nagpur	AML/CFT Regime- Implementation of Post Office saving instruments
	• NACEN, Chennai	Role of FIU, AML & CFT
Feb-12	• NACEN, Faridabad	Presentation on 'Role of FIU and PMLA and Financial Intelligence' during course on 'Commercial Fraud and Money Laundering
	• CBI & Interpol Anti-Corruption Office, Delhi	Lecture on 'Role of FIU-IND in tracing proceeds of crime' during Interpol Global Programme on Anti Corruption and Asset Recovery
	• NACEN, Hyderabad	Lecture on 'Role of FIU for effective implementation of AML & CFT Provisions'
	• Deloitte Touche Tohmatsu India Pvt Ltd, Mumbai	3rd Annual FEMA Summit 2012-FDI Policy and Anti Money Laundering
	• NACEN, New Delhi	FATF-AML/CFT Regime
Mar-12	• FIU-IND, New Delhi	Project FINet-Finex
	• IB, New Delhi	Project FINet-FINex
	• NIPFP, New Delhi	Aadhaar and FATF
	• RTI, Lucknow	Newly recruited ITIs
	• NACEN	PMLA and Role of FIU-IND

Appendix H - Summary of Important FATF recommendations pertaining to Financial Intelligence Units and Reporting Entities.

Recommendation 1 (Assessing risks and applying risk-based approach)

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country.

Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.

Countries should require financial institutions and designated non-financial businesses and professions DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

Interpretive Note

1.1 Countries should understand that the discretion afforded, and responsibility imposed on, financial institutions and designated non-financial bodies and professions (DNFBPs) by the RBA is more appropriate in sectors with greater AML/CFT capacity and experience. This should not exempt financial institutions and DNFBPs from the requirement to apply enhanced measures when they identify higher risk scenarios.

1.2 The general principle of a RBA is that, where there are higher risks, countries should require financial institutions and DNFBPs to take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted. Simplified measures should not be permitted whenever there is a suspicion of money laundering or terrorist financing.

1.3 Supervisors (or SRBs for relevant DNFBPs sectors) should ensure that financial institutions and DNFBPs are effectively implementing the obligations relating to assessment and mitigation of risk.

Recommendation 2 (National co-operation and co-ordination)

Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policymaking and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

Recommendation 10 (Customer due diligence)

Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

Financial institutions should be required to undertake customer due diligence (CDD) measures when:

(i) establishing business relations;

(ii) carrying out occasional transactions: (i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

(iii) there is a suspicion of money laundering or terrorist financing; or

(iv) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The CDD measures to be taken are as follows:

(a) Identifying the customer and verifying that customer's identity.

(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting on-going due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship.

Financial institutions should be required to apply each of the CDD measures under (a) to (d) above, but should determine the extent of such measures using a risk-based approach (RBA).

Where the financial institution is unable to comply with the applicable requirements under paragraphs (a) to (d), it should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

Interpretive Note

10.1 If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing, then the institution should:

(a) identify and verify the identity of the customer and the beneficial owner, irrespective of any exemption or any threshold that might otherwise apply; and

(b) make a suspicious transaction report (STR) to the financial intelligence unit (FIU).

10.2 The CDD measures set out in Recommendation 10 do not imply that financial institutions have to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction. An institution is entitled to rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information.

10.3 Financial institutions may be permitted to establish a business relationship pending verification of the customer under certain circumstances where it is essential so as not to interrupt normal conduct of business. Financial institutions will also need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

10.4 Financial institutions should be required to apply CDD measures to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

10.5 There are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced CDD measures have to be taken. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations (in addition to those set out in Recommendations 12 to 16) include the following:

(a) Customer risk factors:

- ☐ The business relationship is conducted in unusual circumstances (e.g.significant unexplained geographic distance between the financial institution and the customer).
- ☐ Non-resident customers.
- ☐ Legal persons or arrangements that are personal asset-holding vehicles.
- ☐ Companies that have nominee shareholders or shares in bearer form.
- ☐ Business that are cash-intensive.
- ☐ The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

(b) Country or geographic risk factors:

- ☐ Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.
- ☐ Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
- ☐ Countries identified by credible sources as having significant levels of corruption or other criminal activity.

☐ Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

(c) Product, service, transaction or delivery channel risk factors:

☐ Private banking.

☐ Anonymous transactions (which may include cash).

☐ Non-face-to-face business relationships or transactions.

☐ Payment received from unknown or un-associated third parties

Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

- Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

10.6 Where the risks of money laundering or terrorist financing are lower, financial institutions could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors.

Examples of possible measures under simplified CDD are:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).
- Reducing the frequency of customer identification updates.
- Reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold.
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of

10.7 Financial institutions should be required to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of customers.

Recommendation 11 (Record-keeping)

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to 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 criminal activity.

Financial institutions should be required to keep all records obtained through CDD measures (e.g. passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken, for at least five years after the business relationship is ended, or after the date of the occasional transaction.

The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

Recommendation 12 (Politically exposed persons)

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customer or beneficial owner), in addition to performing normal customer due diligence measures, to:

a. have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;

b. obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;

c. take reasonable measures to establish the source of wealth and source of funds; and

d. conduct enhanced on-going monitoring of the business relationship.

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

Interpretive Note

Financial institutions should take reasonable measures to determine whether the beneficiaries of a life insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons. This should occur at the latest at the time of the pay-out. Where there are higher risks identified, in addition to performing normal CDD measures, financial institutions should be required to:

a) inform senior management before the pay-out of the policy proceeds; and

b) conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a suspicious transaction report.

Recommendation 15 (New technologies)

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.

Recommendation 16 (Wire transfers)

Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures.

Recommendation 17 (Reliance on third parties)

Countries may permit financial institutions to rely on third parties to perform elements of CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met:

(a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10.

(b) Financial institutions should take adequate steps to satisfy themselves that copies of relevant documentation relating to the CDD will be made available from the third party upon request without delay.

(c) The financial institution should satisfy itself that the third party is adequately regulated, supervised and monitored.

(d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

Recommendation 18 (Internal controls and foreign branches and subsidiaries)

Financial groups should be required to implement group-wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.

Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing.

Interpretive Note

18.1 Financial institutions' programmes against money laundering and terrorist financing should include:

(a) the development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees;

(b) an on-going employee training programme; and

(c) an independent audit function to test the system.

18.2 The type and extent of measures to be taken should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

18.3 Compliance management arrangements should include the appointment of a compliance officer at the management level.

Recommendation 20 (Reporting of suspicious transactions)

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

Interpretive Note

20.1 All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

20.2 The reporting requirement should be a direct mandatory obligation, and not an indirect or implicit obligation.

Recommendation 21 (Tipping-off and confidentiality)

Financial institutions, their directors, officers and employees should be:

(a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information, if they report their suspicions in good faith to the FIU, and

(b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU.

Recommendation 22and 23(DNFBPs: Customer due diligence)

The customer due diligence and record-keeping requirements set out in Recommendations10, 11, 12, 15, and 17, apply to the following designated non-financial businesses and professions (DNFBPs)in certain situations and in case of transactions of over a prescribed threshold:

(a) Casinos (b) Real estate agents (c) Dealers in precious metals and dealers in precious stones (d) Lawyers, notaries, other independent legal professionals and accountants(e) Trust and company service providers .

Recommendations24 and 25 (Transparency and beneficial ownership of legal persons and legal arrangements)

Countries should take measures to prevent the misuse of legal persons and arrangements for money laundering or terrorist financing. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons or express trusts (including information on the settlor, trustee and beneficiaries) that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares or

bearer share warrants, or which allow nominee shareholders or nominee directors, should take effective measures to ensure that they are not misused for money laundering or terrorist financing. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

Interpretive Note

24.1 As part of the process of ensuring that there is adequate transparency regarding legal persons, countries should have mechanisms that:

(a) identify and describe the different types, forms and basic features of legal persons

(b) identify and describe the processes for: (i) the creation of those legal persons; and (ii)the obtaining and recording of basic and beneficial ownership information;

(c) make the above information publicly available; and

(d) assess the money laundering and terrorist financing risks associated with different types of legal persons created in the country.

24.2 Countries should ensure that either: (a) information on the beneficial ownership of accompany is obtained by that company and available at a specified location in their country; or (b) there are mechanisms in place so that the beneficial ownership of a company can be determined in a timely manner by a competent authority.

In order to meet these requirements, countries should use one or more of the following mechanisms:

(a) Requiring companies or company registries to obtain and hold up-to-date information on the companies' beneficial ownership;

(b) Requiring companies to take reasonable measures to obtain and hold up-to-date information on the companies' beneficial ownership;

(c) Using existing information, including: (i) information obtained by financial institutions and/or DNFBPs, in accordance with Recommendations 10 and 22; (ii) information held by other competent authorities on the legal and beneficial ownership of companies (e.g. company registries, tax authorities or financial or other regulators);and (iii)available information on companies listed on a stock exchange.

24.3 Countries should have mechanisms that ensure that basic information, including information provided to the company registry, is accurate and updated on a timely basis.

24.4 Competent authorities, and in particular law enforcement authorities, should have all the powers necessary to be able to obtain timely access to the basic and beneficial ownership information held by the relevant parties.

24.5 There should be a clearly stated responsibility to comply with the requirements in this Interpretive Note, as well as liability for effective, proportionate and dissuasive sanctions for any legal or natural person that fails to properly comply with the requirements.

24.6 Countries should rapidly, constructively and effectively provide international cooperation in relation to the exchange of basic and beneficial ownership information. This should include (a) facilitating access by foreign competent authorities to basic information held by company registries; (b) exchanging information on shareholders; and (c) using their powers to obtain beneficial ownership information on behalf of foreign counterparts.

Recommendations 26, 27 and 28 (Regulation and supervision of financial institutions and DNFBPs)

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities or financial supervisors should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owner of, a significant or controlling interest, or holding a management function in, a financial institution.

Supervisors should have adequate powers to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose sanctions, in line with Recommendation 35, for failure to comply with such requirements.

Designated non-financial businesses and professions (DNFBPs) should also be subject to regulatory and supervisory measures. This may be performed by (a) a supervisor or (b) by an appropriate self-regulatory body (SRB), provided that such a body can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

Interpretive Note

26.1 A risk-based approach to supervising financial institutions' AML/CFT systems and controls should be adopted so as to allow supervisory authorities to shift resources to those areas that are perceived to present higher risk.

26.2 The assessment of the money laundering and terrorist financing risk profile of a financial institution/group, including the risks of non-compliance, should be reviewed both periodically and when there are major events or developments in the management and operations of the financial institution/group.

26.3 Countries should ensure that financial supervisors have adequate financial, human and technical resources. These supervisors should have sufficient operational independence and autonomy to ensure freedom from undue influence or interference.

Recommendations 29 (Financial Intelligence Units)

Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

Interpretive Note

29.1 At a minimum, the information received by FIU should include suspicious transaction reports, as required by Recommendation 20 and 23, and it should include other information as required by national legislation (such as cash transaction reports, wire transfers reports and other threshold-based declarations/disclosures).

29.2 FIU analysis should add value to the information received and held by the FIU.FIUs should been encouraged to use analytical software to process information more efficiently and assist in establishing relevant links. FIU should conduct both operational analysis using available and obtainable information to identify specific targets and Strategic analysis to identify money laundering and terrorist financing related trends and patterns.

29.3 The FIU should be able to disseminate, spontaneously and upon request, information and the results of its analysis to relevant competent authorities.

29.4 In addition to the information that entities report to the FIU (under the receipt function), the FIU should be able to obtain and use additional information from reporting entities as needed to perform its analysis properly.

29.5 In order to conduct proper analysis, the FIU should have access to the widest possible range of financial, administrative and law enforcement information.

29.6 Information received, processed, held or disseminated by the FIU must be securely protected, exchanged and used only in accordance with agreed procedures, policies and applicable laws and regulations.

29.7 The FIU should be operationally independent and autonomous, meaning that the FIU should have the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and/or disseminate specific information.

29.8 Countries should ensure that the FIU has regard to the 'Egmont Group Statement of Purpose' and its principles for Information exchange between FIUs.

Recommendations 34 (Guidance and feedback)

The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.

Recommendations 35 (Sanctions)

Countries should ensure that there is a range of effective, proportionate and dissuasive actions, whether criminal, civil or administrative, available to deal with natural or legal persons covered by Recommendations 6, and 8 to 23, that fail to comply with AML/CFT requirements. Sanctions should be applicable not only to financial institutions and DNFBPs, but also to their directors and senior management.

Recommendations 40 (Other forms of international co-operation)

Countries should ensure that their competent authorities can rapidly, constructively and effectively (both spontaneously and upon request) provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing.

Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance and should have efficient processes for prioritization and timely execution of requests, and for safeguarding the information received.

Interpretive Note

40.1 Countries should not prohibit or place unreasonable or unduly restrictive conditions on the provision of exchange of information or assistance.

40.2 Exchanged information should be used only for the purpose for which the information was sought or provided. Any dissemination of the information to other authorities or third parties should be subject to prior authorisation by the requested competent authority.

40.3 Competent authorities should maintain appropriate confidentiality for any request for cooperation and the information exchanged, in order to protect the integrity of the investigation or inquiry.

40.4 FIUs should exchange information with foreign FIUs, regardless of their respective status; be it of an administrative, law enforcement, judicial or other nature. To this end, FIUs should have an adequate legal basis for providing cooperation on money laundering, associated predicate offences and terrorist financing.

40.5 Financial supervisors should cooperate with their foreign counterparts, regardless of their respective nature or status. To this end, financial supervisors should have an adequate legal basis for providing cooperation, consistent with the applicable international standards for supervision.

40.6 Financial supervisors should be able to conduct inquiries on behalf of foreign counterparts, and, as appropriate, to authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to facilitate effective group supervision.

40.7 Law enforcement authorities should be able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to money laundering, associated predicate offences or terrorist financing, including the identification and tracing of the proceeds and instrumentalities of crime. Law enforcement authorities should be able to form joint investigative teams to conduct cooperative investigations, and, when necessary, countries should establish bilateral or multilateral arrangements to enable such joint investigations.

40.8 Countries should permit their competent authorities to exchange information indirectly with non-counterparts, applying the relevant principles above. Indirect exchange of information refers to the requested information passing from the requested authority through one or more domestic or foreign authorities before being received by the requesting authority

Appendix I-Mutual Evaluation Report 2010: Rating at a Glance

Rec. No.	Recommendation	Rating
Legal System		
1	Criminalization of money laundering offence	PC
2	Money laundering offence- mental element and corporate liability	LC
3	Confiscation and provisional measures	PC
Preventive measures		
4	Secrecy laws consistent with the Recommendations	C
5	Customer Due Diligence	PC
6	Politically Exposed Persons	PC
7	Correspondent banking	LC
8	New technologies and non face-to-face business	LC
9	Third parties and introducers	N/A
10	Record keeping	LC
11	Unusual transactions	LC
12	Designated Non-Financial Businesses and Professions (DNFBPs)	NC
13	Suspicious transaction reporting	PC
14	Protection and no tipping off	LC
15	Internal controls, compliance and audit	LC
16	Application of R 13,15 and 21 to DNFBPs	NC
17	Effective, proportionate and dissuasive sanctions	PC
18	Operation of Shell Banks	LC
19	Other forms of reporting	C
20	Other NFBP and secure transaction techniques	LC
21	Special attention for higher risk countries	PC
22	Foreign branches and subsidiaries	C
23	Regulation, supervision and monitoring	PC
24	DNFBP- regulation, supervision and monitoring	NC
25	Guidelines and feedback	LC
Institutional and other measures		
26	Financial Intelligence Unit	LC
27	Law enforcement authorities	LC
28	Powers of competent authorities	C
29	Powers of supervisors	LC
30	Resources, integrity and training	LC
31	Co-operation among national agencies	LC
32	Maintenance of comprehensive statistics	LC
33	Unlawful use of legal persons	PC
34	Unlawful use of legal arrangements	PC
International Co-operation		
35	Implementation of international conventions	PC
36	Mutual Legal Assistance and extradition	LC
37	Dual criminality	LC
38	Mutual Legal Assistance on confiscation and freezing	LC
39	Money laundering as extraditable offence	LC
40	Other forms of co-operation	LC

Appendix I- (continued)

FATF Special Recommendations on Terrorist Financing

Spl. Rec. No.	Recommendation	Rating
SR I	Implementation of UN instruments	PC
SR II	Criminalize TF	PC
SR III	Freezing and confiscate terrorist assets	LC
SR IV	Suspicious transaction reporting	PC
SR V	International co-operation	LC
SR VI	AML requirements for money/value transfer service	LC
SR VII	Wire transfer rules	LC
SR VIII	Non-profit organizations	NC
SR IX	Cross-border declaration and disclosure	PC

C- Compliant LC- Largely Compliant PC- Partially Compliant NC- Non Compliant

Appendix J - Outreach

April-11	• Review of AML/CFT Performance of Punjab & Sind Bank, New Delhi. • Review of AML/CFT Performance of Oriental Bank of Commerce, New Delhi • Review of Compliance of SBI & Associate Banks by FIU-IND, New Delhi • Review of Compliance, AML/CFT Policy of Indian Overseas Bank, Chennai • Workshop on Reporting by Indian Overseas Bank, Chennai • Review of AML/CFT Policy & Compliance of Indian Bank Chennai • Workshop on Obligations of Banks at Indian Bank Chennai
May-11	• Workshop on FIUs and their role in detecting economic crime at SBI, Gangtok. • Workshop on compliance under PMLA, 2002 by FIU-India New Delhi
June-11	• Review Meeting with Principal Officers of Indian Private Sector Banks at FIU-IND New Delhi • Workshop on AML/CFT Issues at Kotak Mahindra Bank, Bangalore • Seminar on AML obligations of reporting entities under PMLA at Canara Bank Bangalore • Seminar on AML obligations of reporting entities under PMLA at Vijaya Bank Bangalore • Review of AML compliance of the Bank of Bank of Maharashtra, Pune • Workshop on AML Records Maintenance & obligations of Reporting of Bank of Maharashtra Pune • Workshop on AML Records Maintenance & obligations of Reporting of Bank of Maharashtra Pune • Review of AML Obligations of reporting entity & records maintenance of Canara Bank, Bangalore • AML- Review of Compliance under PMLA of Canara Bank, Bangalore • AML- Review of Compliance under PMLA of Vijaya Bank, Bangalore • Workshop on AML Obligations of reporting entity & maintenance of records of Vijaya Bank, Bangalore • Review of AML Implementation of KYC / AML Standards & Practices of Vijaya Bank, Bangalore • AML Overview of PMLA of UCO Bank Kolkata • AML - Compliance of KYC / AML norms under PMLA by UCO Bank Kolkata • Interaction on AML KYC / AML norms and observance of PMLA of UCO Bank Kolkata • Review of AML Compliance of PMLA by United Bank of India Kolkata • Workshop on AML Best Practices in sound AML and CDD at United Bank of India Kolkata
July-11	• AML- Review of Compliance of PMLA, 2002 by Axis Bank Mumbai • Interaction on AML Reporting obligations of Payment System Operators and New Reporting Format at FIU-IND New Delhi. • Meeting on AML Frauds, Anti-Money Laundering & Compliance at IBA, Mumbai.
Aug-11	• AML- Lecture during Workshop on AML at Kotak Mahindra Bank, Ahmedabad • AML- Lecture during Workshop on AML at Kotak Mahindra Bank, Surat • AML- Lecture during Workshop on AML/CFT issues for Life Insurance Companies at Life Insurance Council Mumbai • AML- Lecture during Workshop on AML/CFT issues for Life Insurance Companies at Life Insurance Council, Mumbai • Meeting on Role of FIU-IND and obligations of Reporting Entities on AML issues under PMLA, Andhra Bank New Delhi • Interaction on AML/CFT Scenario and introduction of new reporting format at FIU-IND, New Delhi • Interaction on AML Compliance of Cooperative Banks to AML/CFT regulations by FIU-IND, New Delhi

Appendix J- (continued)

Sep-11	• AML- Workshop on Red Flag Indicators and New Reporting Format at FIU-IND, New Delhi • Workshop on AML /PMLA - Role of FIU, Obligations of Reporting Entities at NHB, New Delhi • AML- Train the Trainer Workshop on AML/CFT/KYC by FIU-IND New Delhi • Workshop on AML/CFT Regime of India & the compliance requirements of UCB's, RRB's by FIU-IND at CAB, RBI Pune • Workshop on AML Obligations of Reporting Entities of Compliance thereof by UCB's, RRB's & CCB's by FIU-IND at NABARD, Bhubaneshwar • Review of AML-CFT Compliance of ICICI Bank, Mumbai • Workshop on AML-CFT Compliance at ICICI Bank Mumbai
Oct-11	• Workshop on AML / CFT compliance by RRBs & DCCBs bu FIUU-IND at NABARD, Lucknow. • AML- Interface session of Principal Officers of HFCs with FIU-IND at National Housing Bank, Mumbai • Seminar on AML / CFT - FIU Perspective at SBI Academy, Gurgaon • Interaction on AML / CFT framework for Money Changer Association, Chennai.
Nov-11	• AML- Review Meeting of Top 25 MFs by FIU-IND at AMFI, Mumabi. • AML Keynote Address: FATF Guidelines and Expectations at SP Media, Mumbai • Meeting with Public Sector Banks of Western Region on AML framework at Mumbai • Workshop on AML / CFT Obligations of Banks at Nashik • Meeting with Card System Operators at FIU-IND, New Delhi. • Meeting on Role of FIU-IND & AML measures at National Housing Finance, Kerala.
Dec-11	• Annual Meeting of Kolkata based public sector banks on AML issues by FIU-IND at United Bank of India, Kolkata. • AML Lecture during Workshop on AML/CFT issues at Kotak Mahindra Bank, Hyderabad • Lecture on AML- Role of FIU-IND in international Co-operation relating to criminal matters at UNODC New Delhi • Review meeting of Compliance to AML under PMLA regime by UCBs at New Delhi • Lecture on AML/CFT Regime - Obligations of reporting entities at Corporation Bank New Delhi. • Inspection of AML Processing & review of alerts- CBS-Amlock Software at KYC/AML cell of SBI Corporate Center, Jaipur. • Lecture on AML and Role of FIU for effective implementation of AML & CFT provisions at National Academy of Customs, Excise & Narcotics, Kanpur
Jan-12	• Review meeting of Compliance to AML under PMLA regime by Punjab National Bank, Karur Vysya Bank and City Union Bank • AML- Workshop on Red Flag Indicators for Money Transfer Service Agents at FIU-IND, New Delhi • Lecture on FINnet Exchange for senior Income Tax Officers at FIU-IND, New Delhi • Lecture on AML/CFT Regime for Regional Director and Inspecting Officers of National Savings Institute at Nagpur • Lecture on AML and Role of FIU for effective implementation of AML & CFT provisions at National Academy of Customs, Excise & Narcotics, Chennai • Training for Managers of Karur Vysya Bank and City Union Bank on AML/CFT Regime
Feb-12	• Lecture on AML and Role of FIU for effective implementation of AML & CFT provisions at National Academy of Customs, Excise & Narcotics, Faridabad

Appendix J- (continued)

	• Lecture on Role of FIU in Tracing Proceeds of Crime for INTERPOL officials from 15 countries from Asia and South Pacific at New Delhi • Lecture on Role of FIU for effective implementation of AML & CFT provisions at National Academy of Customs, Excise & Narcotics, Hyderabad • Review meeting of Compliance to AML under PMLA regime by State Co-operative Banks at Chennai • Lecture during FEMA Summit 2012 on FDI Policy and AML at Mumbai • Lecture on FATF- AML & CFT regime at National Academy of Customs, Excise & Narcotics, New Delhi • Review meeting of Compliance to AML under PMLA regime by State Insurance Companies at Hyderabad • Meeting with AML Team of IRDA at Hyderabad
Mar-12	• Training of Senior Officers of Banks during 6th Annual Risk and Compliance summit 2012 on AML-Key Policy Changes • Lecture on FINnet Exchange for Officers of Law Enforcement/Intelligece at New Delhi • Lecture on Aadhar and FATF for Govt. Officers at New Delhi • Lecture on Role of FIU for CBDT Officers at Lucknow • Lecture on PMLA and Role of FIU for effective implementation of AML & CFT provisions at National Academy of Customs, Excise & Narcotics, Bangalore • Review meeting of Compliance to AML under PMLA regime by Public Sector Banks at Bangalore • Review meeting of Compliance to AML under PMLA regime by Urban Coop. Banks at Jalandhar • Training of Senior Officers of Banks on AML/CFT Standards and Global Practices-Obligations under PMLA 2002 at Mumbai • Training of Members of CISI and ICSI on combating Financial Crimes at Mumbai

Glossary

AMFI	Association of Mutual Funds in India
AML	Anti Money Laundering
ANMI	Association of NSE Members of India
APG	Asia Pacific Group on Money Laundering
BCP-DR	Business Continuity Plan-Disaster Recovery
CBDT	Central Board of Direct Taxes
CBEC	Central Board of Excise & Customs
CBI	Central Bureau of Investigation
CCR	Counterfeit Currency Report
CFT	Combating Financing of Terrorism
CTED	Counter Terrorism Executive Directorate
CTR	Cash Transaction Report
ED	Enforcement Directorate
EMS	Enterprise Management System
EOI	Expression of Interest
ESW	Egmont Secure Web
FATF	Financial Action Task Force
FEMA	The Foreign Exchange Management Act, 1999
FICN	Fake Indian Currency Notes
FINex	FINnet Exchange
FINnet	Financial Intelligence Network
FIU-IND	Financial Intelligence Unit, India
IA	Intelligence Agency
IB	Intelligence Bureau
IBA	Indian Banks' Association
ICAI	Institute of Chartered Accountants of India
IMF	International Monetary Fund
IRDA	Insurance Regulatory and Development Authority
ISPP	Information Security Policies and Procedures
JWG	Joint Working Group
KMS	Knowledge Management System
KYC	Know Your Customer

LEA	Law Enforcement Agency
MEQ	Mutual Evaluation Questionnaire
MER	Mutual Evaluation Report
MHA	Ministry of Home Affairs
MoU	Memorandum of Understanding
NABARD	National Bank for Agriculture and Rural Development
NBFC	Non-banking Financial Company
NCB	Narcotics Control Bureau
NHB	National Housing Bank
NSCS	National Security Council Secretariat
NTR	Non Profit Organisation Transaction Report
OpWG	Operational Working Group
PDC	Primary Data Centre
PMLA	The Prevention of Money Laundering Act, 2002
R&AW	Research & Analysis Wing
RBI	Reserve Bank of India
RBSC	Reserve Bank Staff College
REIC	Regional Economic Intelligence Committee
RFP	Request For Proposal
RGU	Report Generation Utility
RPU	Report Preparation Utility
RRB	Regional Rural Bank
RVU	Report Validation Utility
SEBI	Securities and Exchange Board of India
SI	System Integrator
STR	Suspicious Transaction Report
UAPA	The Unlawful Activities (Prevention) Act, 1967
UCB	Urban Co-operative Bank
UNSCR	United Nations Security Council Resolution
XML	Extensible Markup Language

"The FIU is to be commended on the effort that it has made over the past year to pick up on the points made in the MER, to monitor the trends in STR filing, and to be proactive in its direct engagement with the reporting institution. The effect appears to have been a markedly improved reporting regime"

Observation of FATF's Team that visited FIU-IND on April 13,2011

Address;
Financial Intelligence Unit - India
6th Floor, Hotel Samrat
Kautilya Marg, Chanakyapuri
New Delhi - 110021

Telephone
91-11-26874429, 26874349, 24672852/53 (EPABX)
91-11-24109791/92/93 (Helpdesk)
91-11-26874459 (FAX)

Website
http://fiuindia.gov.in

Email
helpdesk@fiuindia.gov.in (helpdesk for Project FINnet Gateway Portal)
ctrcell@fiuindia.gov.in (for queries on CTR data quality)
feedbk@fiuindia.gov.in (for feedback)