Financial Intelligence Unit - India

Annual Report
2009-10

सत्यमेव जयते

Department of Revenue
Ministry of Finance, Government of India

Financial Intelligence Unit – India
Annual Report 2009-10

Department of Revenue
Ministry of Finance, Government of India

प्रणब मुखर्जी
PRANAB MUKHERJEE

सत्यमेव जयते

वित्त मंत्री, भारत
FINANCE MINISTER
INDIA

MESSAGE

Financial Intelligence Units play a crucial role in assisting investigating agencies in their endeavour to fight the menace of money laundering and other economic crimes. They also enable intelligence and other agencies to effectively combat financing of terrorism.

India is committed to further strengthen Financial Intelligence Unit – India (FIU-IND) so that it can play a key role in India's Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) regime.

I am happy to learn that FIU-IND is bringing out its fourth Annual Report. I hope that the Annual Report is found useful by all the stakeholders.

(PRANAB MUKHERJEE)

Office : Room No. 134, North Block, New Delhi-110001 Ph. : 23092810, 23092510 Fax : 23093289
Residence : 13, Talkatora Road, New Delhi-110011 Tel. : 23737623, 23323042, 23737658

सत्यमेव जयते

राजस्व सचिव
REVENUE SECRETARY

भारत सरकार
वित्त मंत्रालय
नॉर्थ ब्लाक, नई दिल्ली–110001
GOVERNMENT OF INDIA
MINISTRY OF FINANCE
NORTH BLOCK, NEW DELHI-110001

MESSAGE

Over the last five years, FIU-IND has exhibited its usefulness as a repository of information received from the financial sector. It has also played a crucial role as an interface between the financial sector and investigation/ intelligence agencies, by providing them information on suspect financial transactions. Although the quantum of reports received by FIU-IND has increased manifold over the years, it has been able to effectively handle them.

As part of India's commitment to the global fight against money laundering and terrorist financing, the capabilities of FIU-IND, both in terms of manpower and IT infrastructure, have been substantially enhanced. This would enable FIU-IND to effectively discharge its responsibilities of receiving, analyzing and disseminating the financial information.

I am happy to learn that FIU-IND has been bringing out an Annual Report every year and is now publishing its fourth Annual Report. I hope that the Report is not only a source of information on work completed during the last year, but is also a guiding light for work to be accomplished in the years ahead.

(SUNIL MITRA)

Phone : 23092653, 23092111 Fax : 23092719 E-mail : rsecy@nic.in

Director's Report

Director's Report

During the year 2009-10, Financial Intelligence Unit - India (FIU-IND) completed five years of its setting up. During these five years, FIU-IND has made rapid progress on all fronts and has been able to catch up with much older FIUs in terms of effectiveness and infrastructure. It was decided to commemorate 16th March as FIU-IND Day every year.

The AML/CFT law was further strengthened. The amendments in the Prevention of Money Laundering Act, 2002 (PMLA) that were enacted in February 2009, were brought into force with effect from 1st June 2009. The relevant Rules issued under PMLA were amended twice during the financial year, in November 2009 and in February 2010. Subsequently, another amendment was carried out in June 2010 to further strengthen AML/CFT regime.

FIU-IND continued its focus on enhancing reporting by the financial sector by adopting a multi-pronged approach. Sustained efforts for outreach were continued during the year. 76 workshops were organized for reporting entities at various locations across the country. Over 3,000 representatives from the reporting entities benefitted from these workshops. These outreach activities were organized with the collaboration of Regulators, Industry Associations, as well as individual reporting entities. Efforts were made to focus on specific sectors which needed additional efforts for capacity building. At the same time, compliance activities were strengthened and action was initiated against reporting entities that were found lacking.

During the year, FIU-IND witnessed substantial increase in the number of reports received by it. The number of CTRs increased from 55,11,150 in the previous financial year to 66,94,404 in the year 2009-10. The number of STRs received increased from 4,409 to 10,067 in the current year - a growth rate of over 100%. CCRs also showed a growth of over 250% from 35,730 reports in the previous year to 1,27,781 reports in the current year.

The number of reports analyzed and disseminated also showed commensurate increase. Enhancement of internal capabilities enabled FIU-IND to keep pace with the increased levels of reporting. During the year, FIU-IND's staff strength was enhanced from 43 to 74. FIU-IND also received necessary sanctions from the Government to implement Project FINnet (Financial Intelligence Network) at the cost of over Rs.600 million. Project FINnet will enhance FIU-IND's capabilities to receive, analyze and disseminate intelligence reports. Within the year 2010-11, FIU-IND hopes to put in place a secure mechanism for online submission of reports by

the reporting entities. This will enable near-real time validation of reports as well as immediate feedback to the reporting entities on the quality of reports filed by them.

Our collaboration with the Regulators continued during the year. FIU-IND organized sector specific review meetings jointly with the regulators to monitor compliance to various reporting and other obligations under PMLA. Special attention was paid to money transfer agents and casinos, where reporting obligations were introduced during the year.

FIU-IND also strengthened its relationship with the partner agencies, to enable them to make better use of disseminated intelligence. Apart from organizing meetings and interactions with these agencies, FIU-IND also contributed resource persons for the trainings organized by these agencies in their own training institutes. FIU-IND also signed a Memorandum of Understanding (MoU) with the Directorate of Enforcement to enhance our relationship. More such MoUs would be signed during the coming years.

FIU-IND contributed to the activities of the Egmont Group by participating in the Operational Working Group, Training Working Group and providing inputs for IT working Group. During the year, FIU-IND signed four MoUs with the FIUs of Australia, Canada, USA, and Sri Lanka. MoUs are also under negotiation with many other countries. Our commitment to the international efforts to combat ML/TF would continue.

FATF/ APG Mutual Evaluation Team made an onsite visit to India in November/ December 2009. FIU-IND was closely involved in this evaluation process and in preparation of the Indian response to the Mutual Evaluation Questionnaire (MEQ). FATF Mutual Evaluation Team also visited FIU-IND during its onsite visit. An FIU-IND delegate was also part of the Indian delegation to the FATF meetings. India was admitted as a full member of FATF at the plenary held at Amsterdam in June 2010.

The mutual evaluation process has also thrown up new focus areas for us. We are confident that increased human resources and IT infrastructure would enable us to better our performance in the coming years.

(Arun Goyal)
Director
Financial Intelligence Unit - India

Contents

Performance at a Glance: 2009-10

Collection of information

- 6.69 million Cash Transaction Reports (CTRs) received
- 99.94% CTRs received electronically
- 10,067 Suspicious Transaction Reports (STRs) received
- 1,27,781 Counterfeit Currency Reports (CCRs) received

Analysis and Dissemination of Information

- 9,425 STRs processed
- 7,027 STRs disseminated

Collaboration with domestic Law Enforcement and Intelligence Agencies

- Regular interaction and exchange of information
- Provided information in 344 cases based on requests by agencies

Regional and global AML/CFT efforts

- 84 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

- 76 seminars and training workshops covering 3,145 participants
- Train the trainer programme for AML/CFT capacity building

Improving compliance to the PMLA

- 18 review meetings with Principal officers

Strengthening legislative and regulatory framework

- Regular interaction with the Department of Revenue and regulators

Strengthening IT infrastructure

- System Integrator appointed for Project FINnet

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 and it reads as:

"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 26 of Financial Action Task Force (FATF) also requires countries to establish a FIU to serve as a national centre for receiving, analysing and disseminating Suspicious Transaction Reports (STRs) and other information regarding potential money laundering or terrorist financing.

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 efforts of national and international intelligence, investigation and enforcement agencies in combating money laundering and terrorist financing. It is an independent body reporting to the Economic Intelligence Council headed by the Finance Minister. For administrative purposes, FIU-IND is under the control of Department of Revenue, Ministry of Finance.

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 organization and has a total staff strength of 74 personnel at various levels. The strength of FIU-IND has been enhanced during the year, and these vacancies are in the process of being filled up. Details of manpower in FIU-IND are given in *Appendix A*. The Chronology of various significant events for FIU-IND is at *Appendix B*.

FIU-IND receives prescribed reports on cash transactions, suspicious transactions and counterfeit currency transactions from banks, financial institutions and capital market intermediaries. FIU-IND analyzes the reports received and shares intelligence with its partner agencies specified in Section 66 of PMLA or notified thereunder.

FIU-IND also identifies patterns of money laundering, terrorist financing and other related economic crimes based on the analysis of its various databases. It also maintains a national database of all financial transactions reported to it, and shares this information with enforcement and intelligence agencies on the basis of requests received from them.

Strategic framework of FIU-IND

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

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 to reporting obligations under PMLA
- Building organizational resources
- Strengthening IT infrastructure

The Report analyses the performance of FIU-IND during the year 2009-10 under the above mentioned broad thrust areas.

Visit of Secretary Revenue to FIU-IND on 10th February 2010

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. In addition, 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, and 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 set of provisions – One set of provisions relate to maintenance and submission of information to FIU and the second set of provisions relate 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 provisions relating to maintenance of records and filing of information. The Directorate of Enforcement and its officers are the authority for the provisions relating to search, seizure, confiscation of property etc.

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

Recent amendments to PMLA

PMLA was amended vide the Prevention of Money Laundering (Amendment) Act, 2009, and brought into force with effect from 1st June 2009. By these amendments, the list of predicate offences has been significantly expanded. A new category of offences having cross border implications has been included as predicate offences without any monetary threshold. These amendments have also brought Authorized Persons (dealers in foreign exchange), Payment System Operators and persons carrying on Designated Business or Profession (casinos) within the purview of PMLA as reporting entities.

Amendments to PML Rules

The Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 (the relevant Rules) were amended vide Notification No. 13/2009 dated 12th November 2009 and vide Notification No. 67 dated 12th February 2010.

The salient features of the amendments carried out on 12th November are:

- The definition of 'suspicious transaction' was amended to explicitly include attempted transactions and to make it clear that there is no requirement of threshold for submission of an STR when the suspicion is related to proceeds of an offence. (Rule 2(1)(g))
- All reporting entities are required to maintain and report all transactions involving receipts by non-profit organisations of value more than rupees ten lakh, or its equivalent in foreign currency. (Rule 3(1)(BA))
- It has been explicitly stated that employees of reporting entities are required to keep the fact of

furnishing information in respect of suspicious transactions strictly confidential. (Proviso to Rule 8(3))

- Important amendments in Rule 9 relating to verification of identity of clients are as under:

"(1) Every banking company, financial institution and intermediary, as the case may be, shall,

(a) at the time of commencement of an account-based relationship, identify its clients, verify their identity and obtain information on the purpose and intended nature of the business relationship, and

(b) in all other cases, verify identity while carrying out:

(i) transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or

(ii) any international money transfer operations.

(1A) Every banking company, financial institution and intermediary, as the case may be, shall identify the beneficial owner and take all reasonable steps to verify his identity.

(1B) Every banking company, financial institution and intermediary, as the case may be, shall exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the customer, his business and risk profile.

(1C) No banking company, financial institution or intermediary, as the case may be, shall keep any anonymous account or account in fictitious names.

(2) Where the client is an individual, he shall for the purpose of sub-rule (1), submit to the banking company, financial institution and intermediary, as the case may be, one certified copy of an 'officially valid document' containing details of his identity and address, one recent photograph and such other documents including in respect of the nature of business and financial status of the client as may be required by the banking company or the financial institution or the intermediary, as the case may be.

Provided that photograph need not be submitted by a client falling under clause (b) of sub-rule (1).

(6A) Where the client is a juridical person, the banking company, financial institution and intermediary, as the case may be, shall verify that any person purporting to act on behalf of such client is so authorised and verify the identity of that person.";

(7) (i) The regulator shall issue guidelines incorporating the requirements of sub- rules (1) to (6A) above and may prescribe enhanced measures to verify the client's identity taking into consideration type of client, business relationship or nature and value of transactions.

Every banking company, financial institution and intermediary as the case may be, shall formulate and implement a Client Identification Programme to determine the true identity of its clients, incorporating requirements of sub-rules (1) to (6A) and guidelines issued under clause (i) above."

The salient features of the amendments carried out on 12th February 2010 are:

- Rule 3 sub-rule 1 has been amended and reporting entities are required to maintain records of all transactions and not merely the transactions that are reported to FIU-IND.
- Rule 4 regarding details of information required to be kept in records maintained under Rule 3 has been amended. The records should contain necessary information 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.
- An explanation has been inserted in Rule 9 sub-rule 1A explaining that 'beneficial owner' means the natural person who ultimately owns or controls a client and or the person on whose behalf a transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person.

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 in line with Special Recommendation II of FATF's Recommendations. 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 threshold.

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. 34 entities including entities

covered under UNSCR 1267 and 1373 have been declared as terrorist organizations by MHA under UAPA.

Reporting Entities under PMLA

Banking Companies

- Public sector banks
- Private Indian banks
- Private foreign banks
- Co-operative banks
- Regional rural banks

Financial Institutions

- Financial Institutions as defined in Section 45-1 of the RBI Act
- Insurance companies
- Hire purchase companies
- Chit fund companies
- Housing finance institutions
- Non-banking financial companies
- Payment system operators
- Authorised money changers
- Casinos

Intermediaries

- All entities registered under section 12 of the SEBI Act including:
- Stock brokers
- Sub-brokers
- Share transfer agents
- Bankers to an issue
- Trustees to trust deed
- Registrars to issue
- Merchant bankers
- Underwriters
- Portfolio managers
- Investment advisers
- Depositories and depository participants
- Custodian of securities
- Foreign institutional investors
- Credit rating agencies
- Venture capital funds
- Collective investment schemes including mutual funds

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, Financial Intelligence Unit – India 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.

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, Financial Unit – India 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 a fine under Section 13 for such non-compliance and this fine 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 with within six months from the day 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,

Collection, Analysis and Dissemination of Information

The prime objective of FIU-IND has been combating money laundering, financing of terrorism and economic crime. To achieve this target, FIU-IND has concentrated on effective collection, analysis and dissemination of information.

FIU-IND plays a key interface between the reporting entities and the user agencies. FIU-IND has over the past few years attempted to build in-house capacities for quick analysis and dissemination of intelligence. It has also worked closely with the reporting entities to ensure timely submission of information.

During the current year, the number of reports received, analyzed and disseminated have more than doubled. However, focused attention on thrust areas ensured that quality of reporting was maintained and received reports were analyzed and disseminated in time.

Collect information

Section 12 of the PMLA and rules framed there under require all reporting entities to furnish information to FIU-IND, relating to prescribed cash transactions, suspicious transactions, transactions of forged or counterfeit currency notes and transactions in accounts of non-profit organizations. The formats for submission of information relating to non-profit organizations are in the process of being finalized with the regulators.

Cash Transaction Reports

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

a) All cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency, and

b) All series of cash transactions integrally connected to each other, which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month.

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

Trends in CTRs

- 6.69 million CTRs were reported in 2009-10 as compared to 5.51 million CTRs in the previous year.
- Filing of CTRs in electronic format is increasing. 99.94% of CTRs were received in electronic format in 2009-10 as compared to 99.8% in 2008-09
- CTRs from the smaller banks such as cooperative banks and regional rural banks continue to increase due to technical assistance, training and outreach programs. Reporting entities in these sectors submitted 0.41 million CTRs in 2009-10 as compared to appx.0.33 million in 2008-09

Cash transactions are not permitted in the securities market. IRDA, the insurance regulator has placed restrictions on acceptance of cash for payment of insurance premium. Majority of the CTRs received during the year were from banking companies. As reporting from the larger banks has stabilized, FIU-IND continued its focus on the smaller banks. By providing a Report Submission Utility, FIU-IND has ensured that even the smaller banks such as co-operative banks and regional rural banks submit CTRs in electronic format. This eliminates the possibility of errors in data entry and also ensures that data received is available for search/linking in the FIU-IND database. The quality of reports received is also monitored and feedback is provided to individual reporting entities for improving data quality. During the year, around 6.69 million CTRs have been received *(Table 1)*.

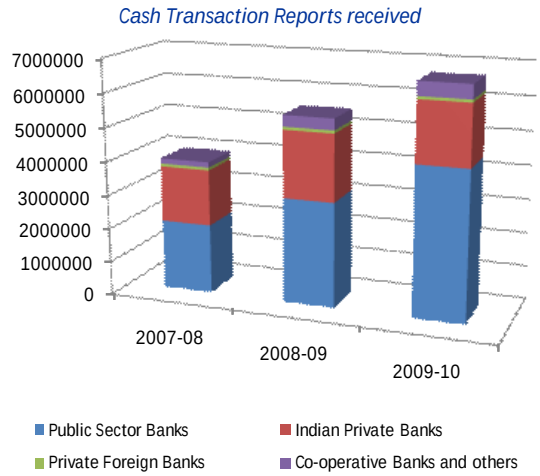


Table 1: Receipt of Cash Transaction Reports

Type of Bank	2007-08	2008-09	2009-10	Till 31st March 2010
Public Sector Banks	20,62,742	31,08,675	44,13,849	1,05,06,863
Indian Private Banks	16,54,749	19,80,045	17,84,665	65,52,597
Private Foreign Banks	84,407	88,239	84,428	3,17,578
Co-operative Banks and others	1,58,015	3,34,191	4,11,462	9,29,197
Total	39,59,913	55,11,150	66,94,404	1,83,06,235
% of Electronic Reports	99.6%	99.8%	99.94%	99.4%

This table shows the number of Cash Transaction Reports (CTRs) submitted by various categories of banks. One CTR covers details of account, related persons and transactions for a month in a bank account.

'Cooperative Banks and others' includes urban co-operative banks, district co-operative banks, state co-operative banks, 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 relevant Rules defines a suspicious transaction as a transaction, whether or not made in cash, which to a person acting in good faith -

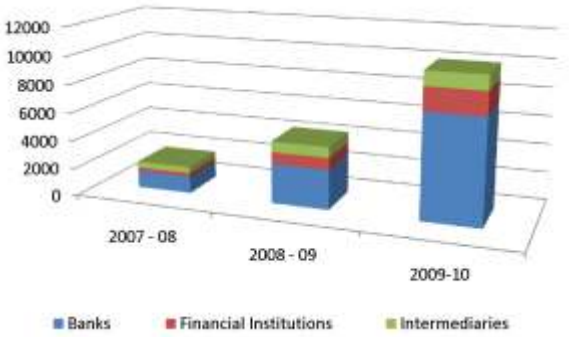
(a) gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime of an offence specified in the Schedule to the Act, regardless of the value involved; or

(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.

Suspicious Transaction Reports received



Trends in STRs

- There was more than 100% growth in STRs received in 2009-10 as compared to 2008-09.
- Number of STRs received from banks showed more than 160% growth in 2009-10 as compared to 2008-09.
- 7394 STRs were received from banks in 2009-10 as compared to 2826 in 2008-09.

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

FIU-IND worked closely with the regulators and the industry associations to develop a common understanding of suspicious transactions and enhancing capabilities of reporting entities to detect and report suspicious transactions. Trainings were organized to enhance awareness and to ensure that even the smaller entities furnished reports in electronic format using the utility developed by FIU-IND. The AML/CFT programs of the larger entities were closely monitored. Regular interactions were arranged with the AML teams of larger entities and sample sanitized cases and typologies were shared. Feedback was also provided on the quality of STRs reported and suggestions for improvement of quality of STRs were provided.

The above thrust resulted in over a 100% growth in STRs reported during the year *Table 2.*

Table 2: Receipt of Suspicious Transaction Reports

Category	2007-08	2008-09	2009-10	Till 31st March2010
Banks	1183	2826	7,394	11,840
Financial Institutions	288	841	1,655	2,872
Intermediaries	445	742	1,018	2,497
Total	1916	4409	10,067	17,209

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

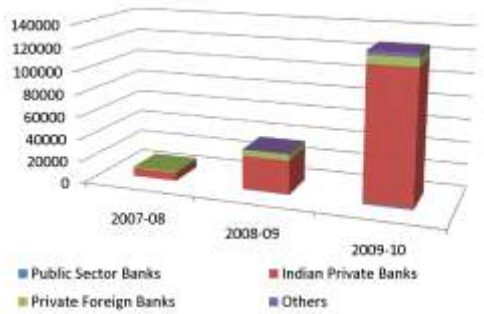
Suspicious Transaction Report on Forged Identity Documents

Reports were received from a bank regarding opening of accounts through introduction by a person alleged to be involved in terrorist activities. It was also reported that the identity proof submitted appeared to be forged and the photograph belonged to the some other person. The reports were disseminated to an Intelligence agency and enquiries confirmed the facts that the introducer was an operative of Indian Mujahideen and had opened accounts in bogus names/addresses with the help of forged documents with the intent of using these accounts in terrorist financing.

Counterfeit Currency Transactions

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 banking regulator, RBI has specified the reporting formats and electronic data structure for submitting Counterfeit Currency Reports (CCRs) vide its circular dated May 22, 2008.

Counterfeit Currency Reports received



Trends in CCRs

- More than 250% growth in CCRs during 2009-10 as compared to 2008-09
- 1,27,781 CCRs received in 2009-10 as compared to 35,730 CCRs in 2008-09 and 8,580 CCRs in 2007-08
- As on March 2010, FIU-IND received information about 1,72,091 incidents of detection of Fake Indian Currency Notes (FICN) with a face value of over Rs10 Crore

During the year, CCR reporting remained a thrust area. 79 advisories were issued to various banks on furnishing of CCRs. Special attention was paid to CCRs during all outreach activity undertaken during the year. Efforts were made to ensure that small incidents of one or two counterfeit currency notes were not missed out and were reported. Workshops were held to train the banks in preparation and submission of reports in electronic format. As a result, the number of CCRs received during the year showed a growth rate of over 250 % *(Table 3).*

Table 3: Counterfeit Currency Reports received

Category	2007-08	2008-09	2009-10	Till 31st March2010
Public Sector Banks	81	396	1,391	1,868
Indian Private Banks	7,388	29,846	1,15,720	1,52,594
Private Foreign Banks	1,111	5,422	7,099	13,632
Others	-	66	3571	3,637
Total	8,580	35,730	1,27,781	1,72,091

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

Process information

Timely processing of information received is one of the key functions of any FIU and it remained a focus area for FIU-IND. The information received from reporting entities was analyzed and linked, and intelligence reports were disseminated to the partner agencies.

Analysis of STRs

Analysis of reports furnished by reporting entities in the financial sector and creation of intelligence reports from this information for the use of partner agencies is a key function of any FIU. FIU-IND 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 process and linking process must result in composite and 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.

Trends in analysis and dissemination of STRs

- Number of STRs processed during 2009-10 was more than 130% higher over the previous year.
- 9,425 STRs were processed during 2009-10 as compared to 4,019 during the previous year.
- 69% of STRs processed were disseminated as compared to 56% in 2008-09 and 47% in 2007-08.

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. Searching and linking of the additional information such as related addresses, individuals, entities and accounts in respect of subjects of STRs was made through a search engine that was developed in-house. The above strategies resulted in better outcomes, even though the number of STRs received by FIU-IND more than doubled during the year as compared to the previous year. Adoption of standard analysis procedures ensured that STRs were carefully analysed by the relevant intelligence group. During the year, 9,425 STRs were processed as compared to 4,019 STRs during the previous year *(Table 4).*

Processing and dissemination of STRs

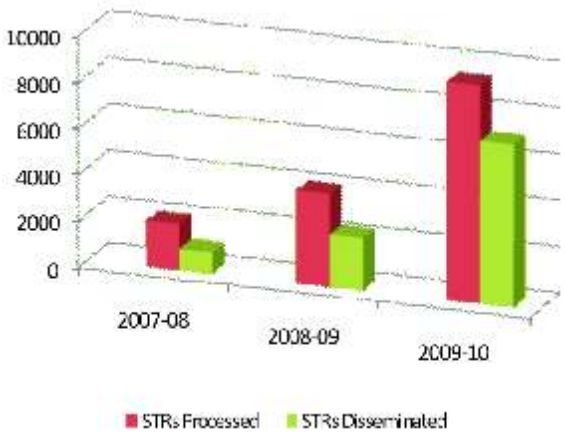


Table 4: Analysis of Suspicious Transaction Reports

Category	2007-08	2008-09	2009-10	Till 31st March2010
STRs received	1,916	4,409	10,067	17,209
STRs Brought forward from Previous Year	171	86	476	--
STRs Processed	2,001	4,019	9,425	16,091
STRs Disseminated	935	2,270	6,571	10,167

This table shows number of STRs received processed and disseminated after analysis.

Suspicious Transaction Report on Money Laundering through Multi-Level-Marketing Schemes

During 2009, STRs were received from banks regarding deposits by many persons in certain accounts in Eastern India and the transfer of the money to other related accounts. The reports also showed that the accounts were connected through common PAN, address and contact numbers. The volume of transactions in these accounts was large and deposits were being made on a daily basis. Money was being deposited by individual investors in the nearby banks and branches using anywhere banking facilities being offered through the Core Banking Solution (CBS) of the banks.

The reports were disseminated to Law Enforcement Agencies, and enquiries revealed that these accounts were being used for Multi-Level Marketing (MLM) activity in the guise of direct selling of consumer goods and services. Very high rates of return had been promised for the deposits, thus luring people to part with funds. In some cases, a large number of cheque leaves had been obtained from the banks, and post-dated cheques for interest and capital repayments had been issued to the investors to give them a false sense of security. Like all pyramid schemes, it was obvious that as the rate of fresh of deposits would reduce, post-dated cheques tendered thereafter would bounce due to inadequate funds being available in the accounts.

Investigations revealed that funds deposited in bank accounts of firms were being transferred to personal accounts of the persons operating the schemes or to current accounts of associate firms. Some of the individuals involved had resigned from the directorship of companies but were still continuing to operate bank accounts and sign cheques.

As per feedback received in FIU-IND, about 15 operators had formed more than 10 firms at various locations such as Kanpur, Mumbai, Chhattisgarh, Jaipur, Indore and Madurai. More than 35 Accounts had been opened in 11 different banks having branches at different parts of the country to make it difficult for the law enforcement agencies to trace the movement of money between these accounts. Rs.130 Crore were transferred over 16 months from the account of one of these MLM firms to the personal account and current account of one of the operators. The cumulative turn-over in these related accounts was more than Rs 300 Crore in a single year.

Crime branch of the state police has attached accounts with deposits of over Rs 190 Crore in different banks in different states. A case of money laundering has also been registered..

STR Trend Analysis

The following trends are observed on the basis of STRs received by FIU-IND during the year 2009-10:

Emerging Trends

- Use of bank account for lottery fraud or employment fraud. The victims were asked to deposit money in bank account which were immediate withdrawn using ATMs
- Use of bank accounts by multi-level marketing (MLM) companies to lure investors for depositing money with the promise of abnormal returns

Declining Trends

- Payment of large amount of insurance premium in cash in one or more polices (The insurance regulator has prohibited collection of insurance premium exceeding Rs 50,000/- in cash)

Continuing Trends

- Use of forged identification documents for opening the account. The identification documents were found to be forged during customer verification procedure. The account holder was not traceable
- Substantial inter-account transfers without any economic rationale between related accounts either controlled by self or through associates
- Topping of credit card by substantial cash and then used for incurring expenses. Cumulative payment during the year was beyond known sources of income
- Frequent cash transactions of value just under the reporting threshold. Cash transactions spilt across accounts to avoid reporting
- Large value cheques deposits in bank account followed by immediate cash withdrawals. Account used for providing fictitious purchase bills
- Name of remitter/ beneficiary matching with watch lists
- Withdrawal of large foreign remittance in cash without any rationale
- Splitting of inward foreign remittances to collect funds in cash in an apparent attempt to avoid fund trail
- Foreclosure of large value housing and auto loans by cash payments
- Use of forged documents for obtaining loans against property from multiple financial institutions
- Payment of substantial premium on one/more policies by multiple Demand Drafts
- Assignment an insurance policy to a third person with no clear relationship to the policy holder
- Large investment in mutual fund using third party cheques without any valid explanation
- Use of multiple folios for investments in mutual funds to avoid linking

Suspicious Circulation of funds without economic rationale

STRs were received from Banks at branches located in a major city in Eastern India. The reports indicated operation of multiple bank accounts in the name of entities belonging to the same person or group of persons. Usually, the accounts were operated by common persons. The accounts also had same proprietor, partners, directors and common addresses. The business activity in most cases had been reported as trading of commodities and investments.

The reports showed cash deposits across the accounts on a daily basis and subsequent transfer of funds to other accounts of the same entity/ group without any economic rationale or logic (Example: cash was deposited in the account of an entity dealing in metals and is transferred to an account of a textile trader and from there to the account of a securities investor and so on). Funds were moved between accounts of the same entity/ groups of entities in a circular manner. The declared business activities of the entities were changed to justify the transactions.

The STRs showed that these entities operated from residential addresses and had a common address, common employees and common contact numbers. Many of the accounts were newly opened. The volume and nature of transactions in these accounts were reported as not commensurate with the business activities and the source of income declared at the time of opening the account.

Analysis of CTR database

FIU-IND has developed in-house a complex search engine that can compare a search string with information in our databases and can generate search results ranked on the basis of degree of match. The search results are arranged in a descending order of rank so that the most relevant results were displayed at the top of the list. This enhances the quality of the searching and linking process 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 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 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 also ensures that all related information available about a subject can be viewed on a single page by an interested analyst. 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 carried out analysis of the CTR database on the request of individual agencies. The CTR data was also processed on the basis of multiple logical criteria and intelligence reports were generated on the basis of data mining and clustering exercises. CTR analysis reports were generated for high-risk scenarios, high-risk geographies and high-risk professions. These analysis reports were found useful by the agencies to whom they were disseminated.

Dissemination

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 system regulators and counterpart FIUs. Statistical information relating to dissemination of intelligence reports during the year 2009-10 is at *Table 5.* Some STRs are disseminated to more than one agency and hence, the number of dissemination reports is higher than the number of STRs disseminated.

Meetings of intelligence groups are conducted at FIU-IND to discuss analyzed reports and decide in which cases the information is fit for dissemination to law enforcement / intelligence agencies for further action, as well as the agency to which such dissemination should be made. Information on regulatory issues was also shared with the concerned regulator.

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 improve quality of reporting.

Dissemination of STRs

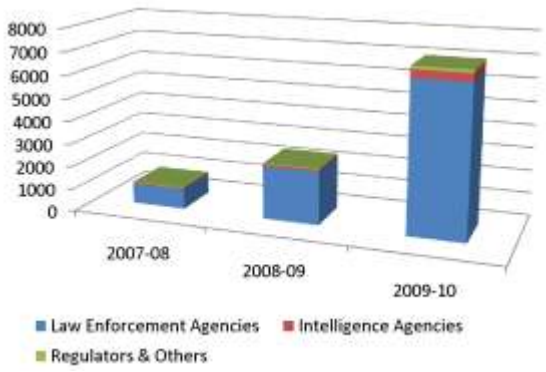


Table 5: Dissemination of STRs

Type of Agency	2007-08	2008-09	2009-10	Till 31st March 2010
Law Enforcement Agencies	885	2319	6,537	10,079
Intelligence Agencies	49	90	362	561
Regulators	34	41	128	233
Total	968	2450	7,027	10,873

This table shows number of disseminations to various types of agencies. Law Enforcement Agencies has the highest share of total dissemination of STRs.

Suspicious Transaction Report pertaining to Foreign Exchange Violations

An STR was received from a bank in respect of a company engaged in the business of renting of cabs. The report disclosed high value inward remittances in the subject's account after October 2008. The remittances of over Rs.1 billion were explained as advance payments of export transactions. The export transactions did not relate to the line of business of the subject, and hence the report was filed. FIU-IND CTR database revealed cash deposits in 4 additional accounts in another bank. The report was disseminated to the relevant law enforcement agencies for investigation.

Another report on the subject was received from another bank showing receipt of funds transferred from other bank accounts. It was also reported that the group company has issued a large number of cheques of small value (less than Rs.10,000/-) in individual names. This report was also disseminated to the relevant Law Enforcement Agency.

Searches conducted by the law enforcement agency revealed incriminating documents and international bank cards issued by foreign banks in the name of the Chairman of the subject entity. Unaccounted cash was also seized during the searches. The investigations revealed fake invoices of local purchase of diamonds of Rs.1.88 billion and no actual purchase of diamonds. In a period of 10 months, the subject entity had received more than Rs.3 billion inward remittances from overseas buyers based in Singapore, Hong Kong and Dubai, alleged to be advance against exports. Investigations revealed that consignees of export shipments were different from the foreign remitters. It was also revealed that the group companies were accepting deposits from public promising high rates of return. Cases were registered against the group companies and its Chairman for violation of Foreign Exchange Management Act.

The outcome of investigation was shared with the State Police to investigate the cheating of public from whom deposits were accepted. Details were also shared with CBDT for investigating evasion of income tax.

Suspicious Transaction Report resulting in detection of large scale bogus billing

Reports were received in 2009 from different reporting entities about the same subject entity. The subject entity is in the securities market business. The reports showed cash deposits in the accounts of the entity followed by transfer of funds to the account of another entity engaged in similar business. Both entities had a common address and a common person was operating both accounts. The reports also showed that a draft was issued in favour of a charitable organization from the account of the related entity but the draft was cancelled and the amount re-credited into the account followed by withdrawal of funds in cash. The amount involved in this transaction was Rs.100 million. FIU-IND CTR database also revealed a number of other bank accounts related to these entities wherein substantial cash transactions were reported. Details of 78 accounts were included and the report was disseminated to CBDT.

CBDT investigated the case and carried out searches in December 2009. Investigations unearthed a wide network across India for laundering of undeclared income through 326 bank accounts opened in various banks. The subject entity was set up by a chartered accountant, who had established various companies/concerns that claimed to conduct share broking activities. In fact, many of the group companies were neither brokers nor sub-brokers.

The group was receiving cash, and this cash was deposited in the bank accounts of various entities of the group. Funds were rotated between accounts to avoid detection and were finally credited in the account of the so called share broking company. This company would issue bills showing fictitious trading in shares and other investments allowing their customers to claim speculative profit or loss. For many accounts, agents had been provided blank signed cheque books to facilitate transactions and commission was charged by the main subject on the basis of transactions taking place in each account. These companies used software that is generally used by stock broker for printing bills for their genuine transactions.

Combating Financing of Terrorism

FIU-IND assists intelligence in combating financing of terrorism in many ways. FIU-IND receives STRs regarding suspected financing of terrorism. The definition of 'suspicious transaction 'in the relevant PMLA Rules specifically provides for reporting of suspect transactions relating to terrorist financing . FIU links such STRs of suspected financing of terrorism with information available in its other databases and analyses the reported suspicion. In cases, where underlying suspicion is related to terrorist financing, information is disseminated to intelligence agencies.

FIU-IND also supports the efforts of intelligence agencies on suspected terror financing by providing information specifically requested by them, either by searching its database or by obtaining specific information from the reporting entities.

FIU-IND is a member of the Egmont Group of FIUs and is regularly sharing information with foreign FIUs over Egmont Secure Web on suspected money laundering and terrorist financing cases. FIU-IND has entered into MoUs with 11 foreign FIUs for furthering cooperation and exchange of information to combat money laundering and terrorist financing, and MoUs are also under negotiation with more than FIUs.

Financial institutions (reporting entities) are often the front-line defence 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 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 .

PMLA has been amended and new categories of reporting entities such as payment system operators (money transfer service providers, card system operators etc.) and authorized money changers have been included as reporting entities under PMLA w.e.f 1st June 2010. The number of TF related STRs have increased substantially after Money Transfer Service Operators were brought under the PMLA regime in June 2009 .

FIU-IND has shared various red flag indicators with reporting entities to help detect suspicious transactions (including TF STRs) Some sample indicators are :

- Match of customer details with known terrorists or persons linked with terrorist organizations. (watch lists or person reported in media/open source)
- Customer who receives transactions in a pattern consistent with financing of terrorism.

Suspicious ATM Withdrawals

A report was received from a bank of transactions in a saving account in a district in Kerala. The account showed cash deposits below Rs. 50,000/- across several branches in Kerala and Maharasthra, followed by withdrawals through ATMs. The report was disseminated to an Intelligence Agency in February 2009. Enquiries revealed that the subject had gone to one of the gulf countries for employment and had started his own business in flowers and curtains in Kerala on his return. Analysis of two bank accounts of the person and his son revealed remittances from gulf and immediate cash withdrawal from an ATM at Hyderabad. Investigations showed business connections with an accused who was in police custody for involvement in a pipe bomb case. The money was withdrawn form Hyderabad based ATMs by an associate of the accused and was allegedly used to facilitate terrorist activities.

- Transaction involving a jurisdiction/area considered to be high risk from the terrorist financing perspective.

During outreach meetings with reporting entities, FIU-IND shares current TF "scenarios" based on current trends and techniques identified through STRs and other means. During sector specific STR review meetings, the red flag indicators for TF cases are discussed and possible areas of improvement are identified.

Individual review meetings are held with important reporting entities to review their CFT related procedures, roles and responsibilities, training plan, activated scenarios and future roadmap.

FIU-IND has conducted analyses of CTRs and other transactions relating to localities with high TF risks and the results have been shared with intelligence agencies.

The statistics of STRs disseminated to and information provided in response to requests for information received from the intelligence agencies (IAs) is as under:

	07-08	08-09	09-10	Till 31st Mar 2010
Dissemination of STRs to IAs	49	90	362	561
Requests for information received from IAs	87	190	226	543

Project FINnet (Financial Intelligence Network) would enhance the efficiency and effectiveness in FIU-IND's functions, including identification of TF related STRs.

Suspicious Transaction Report with possible links to Terrorist Financing

An STR was received from a bank of a person residing in Western UP, who had opened an account declaring his profile as self employed (trader) with gross annual income of Rs 3 lakh. The account showed small cash deposits from different locations such as Jammu, Srinagar, Mahrajganj, etc. and the proceeds were withdrawn immediately from ATMs located in UP and Delhi, which was considered suspicious by the reporting bank. The report was sent to Intelligence Agencies in February 2009. Enquiries by Intelligence Agencies revealed that the subject owned a factory at Jammu and had business dealings in Srinagar, but it was also revealed that one of his relatives residing in UP had links with terrorists and had undergone imprisonment in Guwahati Jail.

Domestic and International Cooperation - Building Partnerships

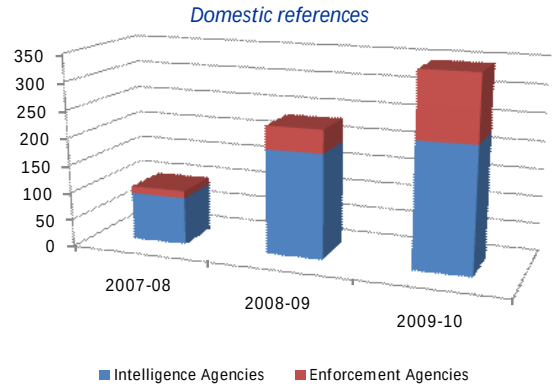
FIUs act as an interface between the financial sector and the law enforcement and intelligence agencies. At FIU-IND, emphasis is placed on maintaining and improving operational relationships with the partner agencies. Such relationships extend beyond mere dissemination of intelligence reports.

During the year, FIU-IND maintained close professional relationship with partner agencies based on mutual trust and understanding. FIU-IND adopted best practices of exchange of information to enhance its ability to respond faster to the requirements of partner agencies. Close relationship with regulators also facilitated further strengthening of AML and CFT regime in India.

Law enforcement/intelligence agencies

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 based on analysis of STRs. FIU-IND also provideds them with additional financial information available in its databases on request.

In order to enhance the operational relationships with the partner agencies, FIU-IND appointed its officers as nodal officers to deal with all issues relating to individual agencies. Partner agencies were also encouraged to appoint nodal officers who remained in constant communication with FIU-IND. Such relationships augmented the structured interactions and enhanced the quality of understanding with agencies. Through regular two-way communication between nodal officers, FIU-IND was able to better understand the requirements of partner agencies. Two meetings were organized during the year with the nodal officers of 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 to various agencies. FIU-IND also interacted with the nodal officers of law enforcement agencies of the state governments and union territories. Two meetings were organized in Delhi with the nodal officers of the state governments to highlight the areas where there could be better cooperation on AML/CFT issues and curbing of economic crimes.

FIU-IND's database on cash and suspicious transactions have been found to be 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 ongoing investigations. During the year, FIU-IND provided timely information to various agencies in response to 344 references on money laundering, terrorist financing, corporate frauds, organized crimes, fake Indian currency, tax evasion etc. *(Table 6).*

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

During the year 2009-10, 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 entered into an MoU with the Directorate of Enforcement, the agency that undertakes investigations and prosecutions under PMLA. MoUs are also being negotiated with other partner agencies, and more such MoUs will be entered into in the coming years.

Signing of MoU with Directorate of Enforcement on 20th Nov. 2009

Table 6: Domestic references from law enforcement/ intelligence agencies

Category	2007-08	2008-09	2009-10	Till 31st March 2010
Requests received from intelligence agencies	87	190	226	543
Requests received from law enforcement agencies	13	42	118	173

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

Regulators

FIU-IND has also developed close relationship with financial system 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 ensured that suitable modifications were carried out in the circulars, wherever necessary.

FIU-IND continued its regular interaction with the regulators, industry associations and Self Regulatory Organisations to develop a common understanding of obligations under PMLA, and improve compliance to AML norms & reporting obligations under PMLA. FIU-IND also interacted with regulators for identification of legal provisions requiring amendment, issues requiring clarification/ intervention and 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

The fight against money laundering and financing of terrorism is a global effort. FIU-IND contributed by actively participating in the efforts of the international community. FIU-IND also adopted a strategy of building healthy relationships based on trust and cooperation with its counterpart FIUs of other countries. Information was shared with foreign FIUs on regular basis. Three more MoUs were signed during the year and more MoUs are under negotiation with other FIUs. FIU-IND also contributed to the activities of regional and international bodies dealing with AML/CFT issues.

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 also ensures adherence to its standards by making sure that countries across the world bring about legislative and regulatory reforms in these areas. It further monitors the progress of the anti-money laundering efforts of its members.

Since it was established by the G-7 Summit in Paris in 1989, FATF has worked towards preventing the abuse of the financial system by criminals. The initial task of FATF was to examine money laundering techniques and trends, review action being taken to combat money laundering, and set out the steps that are still needed to prevent abuse of the financial system by money launderers. It developed a set of Forty Recommendations in April 1990 that form the standards as well as an action plan for preventing and combating money laundering. These recommendations were revised in 1996 and again in 2003.

In 2001, FATF's scope was broadened and the combating of terrorist financing came into focus. In October 2001, FATF came out with Eight Special Recommendations to tackle terrorist financing. In October 2004, it came out with a ninth Special Recommendation, leading to the present set of the 40+9 Recommendations. Some of the important recommendation relating to FIUs and their working are at *Appendix H.*

The initial Task Force set up in 1989 included representatives from the G-7 member States, the European Commission and eight other countries. As on 31st March, 2010, FATF had 33 jurisdictions and 2 regional organizations (European Commission and Gulf Co-operation Council) as its members apart from one jurisdiction as an observer member (India). It also had 8 FSRBs (FATF Style Regional Bodies) as its associate members, and 21 international bodies as observer members.

FATF promotes the adoption and implementation of measures to combat money laundering and terrorist financing globally. It develops typologies of money laundering and terrorist financing methods, trends and techniques. It also undertakes mutual evaluation of the legal and financial system of its member countries to ensure adherence to its recommendations.

FIU-IND 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 at Paris in October 2009 and at Abu Dhabi in February 2010.

Visit of JAFIC delegation to FIU-IND in February 2010

FATF Mutual Evaluation

The FATF evaluation of India took place during the months of November and December 2009. FIU-IND was also actively involved in the preparation of the Indian response to the Mutual Evaluation Questionnaire (MEQ) mutual evaluation of India, as well as in various onsite meetings organized for interaction of FATF/ APG Evaluation Team with different Indian agencies. The FATF/ APG Mutual Evaluation Team, that made onsite visit to India, also visited FIU-IND on 1st December 2009. FIU-IND officials were also closely involved in the Evaluation Team's meetings with Designated Non-Financial Businesses & Professions (DNFBP) sector i.e Casinos, Accountants and Lawyers.

Egmont Group of FIUs

The Egmont Group of FIUs is an informal group of FIUs for 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.

As on 31st March 2010, the Egmont Group had 117 FIUs as its members. Member FIU undertake to subscribe to the Egmont Group principles. The member FIUs work for co-operation and exchange of information with other Egmont Group FIUs on the basis of reciprocity or mutual agreement. They follow the basic tenets laid in the Egmont 'Principles for Information Exchange'.

Egmont principles envisage free exchange of information between FIUs for purposes of analysis and respect for confidentiality. The information exchanged under Egmont Principles is used for intelligence purposes only and cannot be used for any other purpose without prior consent of the providing FIU.

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 Annual Plenary session of Egmont at Doha, Qatar in May 2009, and the Egmont Working Group meetings at Kuala Lampur, Malaysia in October 2009 and Port Louis, Mauritius in March 2010. FIU-IND officials have been actively participating in various working group meetings, particularly in Operational Working Group (OpWG), Training Working Group (TWG) and IT Working Group (ITWG).

Co-operation and exchange of information with other FIUs

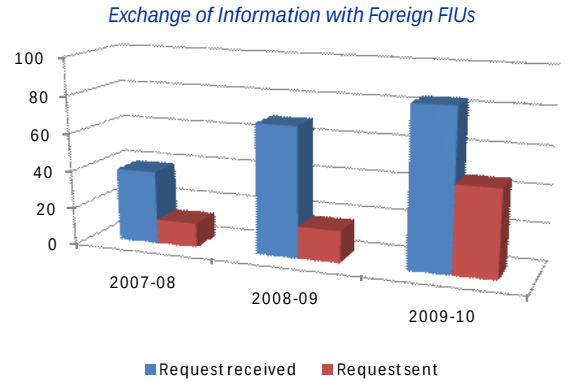
FIU-IND adheres to the Egmont principles of free exchange of information. All requests for information are replied to, in time, including cases where no information can be found.

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 at *Table 7.*

Table 7: Exchange of information with foreign FIUs

Status of Action Taken	2007-08	2008-09	2009-10	Till 31st March 2010
Request received from foreign FIU	39	69	84	206
Request sent to foreign FIU	13	17	46	78

This table shows number of requests for information received and sent to foreign FIUs. After June 2007, all such requests were made and received using Egmont Secure Web.



Signing of MoU with FINTRAC, FIU of Canada at Kuala Lampur, Malaysia

MoUs with foreign FIUs

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 MoUs with various FIUs during the year. MoUs with the FIUs of Australia, Canada, United States of America and Sri Lanka were signed during the year. Signing of MoUs with Australia and Canada were significant as both these countries require an MoU before exchange of information. MoUs with more than 30 countries are under various stages of negotiation (*Table 8).*

Table 8: MoUs with Foreign FIUs

FIU & Country	MoU signed on
Financial Intelligence Unit, Mauritius	11.02.2008
Anti-Money Laundering Council, Philippines	11.03.2008
Conselho de Controle de Atividades Financeira, Brazil	27.05.2008
Unit Perisikan Kewangan, Bank Negara Malaysia, Malaysia	21.10.2008
Federal Service for Financial Monitoring, Russia	05.12.2008
Australian Transaction Report & Analysis Centre, Australia	26.05.2009
Financial Transactions and Reports Analysis Centre, Canada	21.10.2009
Financial Crimes Enforcement Network, USA	03.03.2010
Financial Intelligence Unit, Sri Lanka	26.03.2010

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. Through the mechanism of JWGs on Counter terrorism, FIU-IND has been able to establish one to one relationship with counterpart FIUs and other relevant law enforcement and intelligence agencies in many countries.

These Working Groups are normally serviced by the Ministry of External Affairs. During the year, FIU-IND participated in the meetings of the Joint Working Group on Counter Terrorism with EU in June, 2009.

Raising awareness and building capacities of reporting entities

The success of an FIU depends not only on its ability to link and analyse information, but it also depends on the ability of reporting entities in effectively identifying and reporting suspect transactions. Enhanced awareness of AML norms among different staff of the reporting entities and close monitoring of transactions to adhere to PMLA obligations has a deterrent effect on attempts to launder money or financing activities of terrorism.

Realizing that reporting entities play an important role in combating abuse of the financial system, FIU-IND adopted a twin strategy for enhancing compliance of reporting entities to their obligations. On one hand, the focus was on increasing awareness about their reporting obligations under PMLA and building their capacities. On the other hand, various monitoring mechanisms were put in place to ensure better compliance to PMLA.

Building capacities and raising awareness among the reporting entities is the first step towards effective deterrence. FIU-IND worked towards raising awareness among reporting entities of their reporting obligations and making them realize about the role they can play in combating money laundering and financing of terrorism.

FIU-IND adopted a multi-pronged strategy to enhance awareness. The Internet was used to make information on AML easily available on FIU-IND's website. Seminars and workshops were organized across the country to spread awareness on AML/CFT issues among all levels of personnel of reporting entities. Resource persons were provided for seminars and workshops organized by regulators, industry associations, professional bodies and individual reporting entities. A 'Train the trainers' workshop has been organized by FIU-IND every year to create master trainers. Training material prepared by FIU-IND is being made available to all reporting entities to conduct their own training seminars.

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

As part of its outreach program, FIU-IND provided resource persons for various AML/CFT seminars organized for capacity building among reporting entities. During the year, FIU-IND participated in 76 workshops/interactions on AML/CFT awareness in collaboration with regulators, industry associations, professional bodies and reporting entities, targeted at over 3,100 participants. The statistics relating to training seminars and workshops are at *Table 9.*

The regulators such as Reserve Bank of India and NABARD organized training workshops for the principal officers, technical and operational staff of reporting entities for better compliance to AML/CFT norms. After concentrating on enhancing AML awareness among the larger reporting entities in the past, during the year, FIU-IND focused on enhancing awareness among Urban Co-operative Banks (UCBS), Regional Rural Banks (RRBs) and Capital Market Intermediaries.

Onsite workshops were organized targeting not only top management and principal officers of reporting entities, but also operational staff at smaller locations across the country. Such workshops and seminars included sessions on AML legislation, identification and reporting of suspicious transactions, as well as demonstrations on use of software utilities developed by FIU-IND for preparation of reports in electronic format, particularly by smaller entities that lack sophisticated IT infrastructure.

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

'Train the Trainers' Workshop

A 'Train the Trainers' workshop was organized by FIU-IND in October 2009 at India Habitat Center, New Delhi. This workshop has been organized once every year with the objective of increasing the availability of in-house trainers among reporting entities. This program was attended by 56 key resource persons and trainers of PSU Banks, Private Indian Banks and Regulators. The workshop has been effective & popular Similar workshops are planned for the coming years.

Participants at the 'Train the Trainers' Workshop in October 2009

Table 9: Outreach Activities

Outreach Activity	Number of Interactions			
	2007-08	2008-09	2009-10	Till 31st March 2010
Seminars and Training workshops	93	103	76	329
Number of Participants	5,479	3,617	3,145	14,990

Ensuring Compliance to reporting obligations under PMLA

Apart from enhancing awareness of AML/CFT issues at all levels, FIU-IND has also focussed on effective monitoring and enforcement of compliance to reporting obligations under PMLA.

Although the initial efforts of FIU-IND were aimed at improving awareness at all levels of reporting entities and assisting them in submitting electronic reports, the subsequent efforts have focused on ensuring compliance.

The strategy adopted was of focused review meetings with principal officers of sector specific reporting entities in a group as well as interaction with individual reporting entity to provide guidance and feedback on its systems as well as on the quality of reports. FIU-IND's Annual Report and Newsletters were used to share information on high risk scenarios with reporting entities to enhance their reporting. At the same time, information on compliance by individual entities as well as sectors was shared with regulators for furthering compliance to PMLA.

Review meetings

FIU-IND adopted a practice of periodic sector-wise reviews to evaluate the AML performance of specific reporting entities as well as sectors *Table 10*. These review meetings were held with principal officers of reporting entities and representatives of regulators were invited to participate so that industry-specific issues could be examined in detail. Sector-specific meetings also enabled FIU-IND to evaluate the AML performance of individual reporting entities as compared with their peers.

Table 10 -Review Meetings with Principal Officers

May 2009	• Registrars & Transfer Agents • Asset Management Companies
Jun 2009	• Life Insurance Companies
Jul 2009	• Public Sector Banks
Aug 2009	• Casinos • Regional Rural Banks
Sep 2009	• Urban Cooperative Banks • Regional Rural Banks • Stock Brokers • Private Sector Banks
Jan 2010	• Housing Finance Companies • SBI and its Associate Banks
Feb 2010	• Life Insurance Companies • Regional Rural Banks • Casinos • Urban Cooperative Banks • Asset Management Companies/ Registrars & Transfer Agents • Foreign Banks

During these review meetings, number and quality of reports submitted by individual reporting entities were analyzed to assess gaps and to identify focus areas. Examples of sanitized cases and feedback received by FIU from law enforcement and intelligence agencies were also shared during these meetings. In some meetings, reporting entities were also asked to make presentations on their AML/CFT systems so that the other reporting entities could learn from the experiences of their peers.

Other compliance measures

FIU-IND has also created a compliance section to act as a nodal point for examining compliance and for taking corrective action for specific cases of suspected 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 from external sources was used to identify suspected cases of non-compliance in reporting obligations. Information culled out from STRs was used to examine if other reporting entities involved in transactions have examined and reported these transactions. Information was also obtained from reporting entities to identify suspected cases of non-compliance. As a first step, advisories were issued to reporting entities highlighting problem areas and suggesting corrective action. Reporting entities suspected of lagging behind were selected for prima facie review on the basis of comparison of their performance with their peers. After monitoring of the performance of these reporting entities under review, a view was taken whether the reporting entity has shown improvement or whether a notice is to be issued for levy of fine for non-compliance under section 13 of PMLA.

During the year, 237 reporting entities were issued advisories to improve their compliance under PMLA. Notices were issued to five banks proposing to impose fine for suspected failure to comply with its reporting obligations, particularly in filing CTRs and STRs.

Organizational Capacity Building

Financial Intelligence Units have to keep pace with the dynamic and ever-changing world of crime. Criminals and money-launderers keep developing new techniques to evade detection. FIU-IND analysts have to keep developing their skills to remain effective.

Motivational talk at FIU-IND day on 16th March 2010, the occasion of completion of five years of its operation

FIU-IND made proactive efforts to regularly upgrade the skills of its employees by providing them

Table 11: Capacity building workshops attended by officers from FIU-IND

Month	Workshop	Organized by	Place
Apr 2009	Regional workshop on abuse of charitable and non-profit organizations	US Treasury	New Delhi
Aug 2009	Workshop on Intelligence gathering and Intelligence tradecraft	Central Economic Intelligence Bureau	New Delhi
Aug 2009	Workshop on corporate frauds	Indian Institute of Corporate Affairs	New Delhi
Aug 2009	Seminar on Commodity Futures Market	Indian Institute of Capital Markets	New Mumbai
Sep 2009	AML/CFT Workshop	US Treasury	New Delhi
Sept-Oct 2009	South Asia Regional Workshop on AML/CFT	AUSTRAC	New Delhi
Oct 2009	Seminar on Commodity Futures Market	Indian Institute of Capital Markets	New Mumbai
Nov 2009	Workshop on Policy Development	India-IMF Training Program	Pune
Nov 2009	IMF workshop on Financial Sector Supervisors	India-IMF Training Program	Pune
Nov 2009	Mutual Evaluation Assessor Training	FATF	Toronto
Feb 2010	Workshop on supervision of Securities Market	AUSTRAC	New Delhi

opportunities for training on AML/CFT and related economic issues. During the year, FIU-IND officials attended training programs on various economic issues including securities markets, commodity markets, corporate frauds, abuse of charitable and non-profit organizations, financial sector supervision and AML policy development etc. (*Table11)*.

FIU-IND is also a national resource centre on AML/CFT issues. It has compiled material on money laundering, terrorist financing and related economic issues.

Strengthening IT Infrastructure

FIU-IND continued its sharp focus on use of Information Technology as a tool to enhance performance. During the year, FIU-IND received approval for Project FINnet, which will greatly enhance the IT capabilities of FIU-IND. The project entails an approximate cost of Rs.60 Crore (Rs.0.6 billion) and includes upgradation of hardware and software as well as its maintenance over the next five years.

Assistance to smaller reporting entities

Smaller banks such as cooperative banks and regional rural banks do not have centralized databases, and hence, face difficulties in preparing and submitting CTRs in electronic format. A Report Preparation Utility (RPU) developed by FIU-IND is available for free download on the FIU-IND website, and is of immense assistance to smaller reporting entities in generation of reports in electronic format. This utility has features for data entry; validation of data fields; and export of data into the prescribed data structures. The availability of the report preparation utility and outreach activities for the smaller reporting entities reduced the number of manual reports from 15,470 in the year 2007-08 to 9,001 in the year 2008-09 to less than half at around 4,000 in the year under report. As a result, the percentage of electronic reports increased from 99.84% to 99.94% in the current year.

Availability of reports in electronic format enables their quick updating in the FIU-IND databases and eliminates the possibility of any errors in data entry of manual reports at FIU-IND.

Data quality

Effective search and analysis is dependent on the quality of data available in reports submitted by reporting entities. FIU-IND has developed a data validation utility to check the reports received from reporting entities. This utility identifies different types of data defects on the basis of in-built data validation rules and also generates a data quality report summarizing the types of defects noticed in each report.

A data quality sheet is prepared by this utility for each report received and indicates the particular file, record number and field in which a data quality defect is noticed. During the year, these data quality reports were sent electronically to reporting entities for each report received by FIU-IND. If the defects were minor, the reporting entity was asked to ensure that the errors were not repeated. In case of serious errors, the reporting entity was also advised to re-submit the report after removing the data defects pointed out.

Monitoring

During the year, FIU-IND conducted an exercise to identify Cash Transaction Reports (CTRs), which though submitted in correct data structure, contained information that appeared to be in the nature of outliers. All such outliers were communicated to the individual reporting entities for verification. In cases where the reporting entities found errors, correct data was re-submitted after verification. This helped in capacity building within the organization and increased awareness amongst reporting entities regarding accuracy and correctness of reports, apart from enhancing the results obtained in the linking and analysis process.

Search and linking of data

FIU-IND has developed in-house a complex search engine that can compare a search string with information in our databases and can generate search results ranked on the basis of degree of match. The search results are arranged in a descending order of rank so that the most relevant results are displayed at the top of the list. This enhances the quality of the 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 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 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 also ensures that all related information available about a subject can be viewed on a single page to an interested analyst. 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.

This year FIU-IND also designed an application for allowing multiple text strings to be searched at the same time, thus reducing the time taken in searches and enhancing the quality of search results.

Project FINnet

Key objectives

Financial Intelligence Unit – India (FIU-IND) initiated project FINnet (Financial Intelligence Network) 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".

The components of Project FINnet are:

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

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

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

iv) Building 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) Adopting 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.

The Project consists of two phases i.e. Design phase and Implementation phase. In 2007, M/s Ernst & Young Pvt. Ltd. (E&Y) were selected as Consultants for the Project FINnet. During the Design Phase (2007-08), the functional and technical specifications for Project FINnet were finalized in active consultation with FIU-IND and other stakeholders.

Signing of contract with System Integrator M/s WIPRO on 25th Feb 2010

Outcomes of Project FINnet

Project FINnet would substantially enhance the efficiency and effectiveness of FIU-IND's core function of collection, analysis and dissemination of financial information. IT enablement of key processes would ensure substantially higher productivity, faster turnaround time and effective monitoring in all areas of FIU-IND's work. This Project, once fully implemented, is expected to result in the following broad outcomes:

- Advanced utilities to prepare, validate and encrypt electronic reports in XML format
- Online secure gateway to receive reports
- Scanning and extraction of data from manual reports
- Streamlined process for data quality validation and feedback
- Rule based checks for insufficient information using customized dictionaries
- Advanced de-duplication to overcome name and address variations
- Identification of both explicit and implicit relationships

- Rules based systems to assign risk and prioritize alerts
- Automated advanced search and resolution before the case is made available to the analyst
- Automated application level access
- Secure role based access
- Automated detection of suspicious transaction patterns using data mining tools
- Advanced trend analysis using Business Intelligence tools

Status

During the year, M/s Wipro Ltd. was selected as the System Integrator (SI) for Project FINnet. The SI would set up the IT systems and related infrastructure based on the design documents, during the implementation phase that started in February 2010. The Consultant (Ernst & Young) would provide project management services during the implementation phase. SI would be responsible for development / customization, integration, testing and rollout of software applications and other infrastructure at FIU-IND office location, Primary Data Centre (PDC) and Business Continuity Plan-Disaster Recovery (BCP-DR) sites. The total project timeframe is 5 years, of which the timeline for validation and acceptance of the complete software solution is two years from the date of contract (25th February 2010). SI would provide support for software and hardware for 3 years from the date of acceptance of the software solution.

The project timelines in the implementation phase are as under:

Interaction with the representatives of Law Enforcement Agencies/ Intelligence Agencies on Project FINnet in March, 2010

Phase	Description	Expected Completion Time
Phase I	Collection Systems	T + 7 Months
Phase II	Analysis and Dissemination Systems	T + 12 Months
Phase III	Risk Management and Advanced Systems	T + 15 Months
Phase IV	Validation & Acceptance	T + 24 Months (T2)
Phase V	Enhanced Support	T2 + 12 Months
Phase VI	Maintenance Support	T2 + 36 Months

T : Effective date of contract = 25th Feb 2010
T2 : Date of acceptance of complete solution

During the year, FIU-IND also organised interaction with the representatives of Law Enforcement Agencies and intelligence Agencies to present and discuss implementation road map of project FINnet.

Appendices

Appendix A – Staff strength of FIU-IND

Post	Sanctioned Strength	Working as on March 31, 2010
Director	1	1
Additional Director	10	5
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)	20	9
Assistant Director Systems (earlier System Analyst/ Programmer)	6	4
Section Officer	2	1
Others*	31	14
Total	74	36

**includes persons hired 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

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 USA
Mar 16, 2010	FIU-IND Completes 5 years of its setting up
Mar 26, 2010	Signed MoU with Sri Lanka

Appendix C – Predicate offences under PMLA

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	Amends rule 2, 3, 5, 6,7, 8, 9 and 10 of the Rules notified by Notification No. 9/2005.
12.02.2010	7/2010	Amended requirements of maintenance of accounts and definition of beneficial owner.

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

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
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
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
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

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 (Account based relationship)	At the time of commencement of account-based relationship
Verify the identity of the client (Non-account based relationship)	At the time of carrying out a transaction for an amount equal to or exceeding Rupees fifty thousand or any international money transfer operation
Where the client is acting on behalf of a beneficial owner, identify the beneficial owner and take all reasonable steps to identify his identity.	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	Within 7 working days from the date of transaction
Furnish report in respect of Non-Profit-Organizations (NPOs)	Within 15th day of succeeding month (Monthly Reporting)
Furnish Suspicious Transaction Report (STR) to FIU-IND containing details of all suspicious transactions whether or not made in cash, including attempted suspicious transactions	Within 7 working days on being satisfied that the transaction is suspicious
Maintain records of identity of clients	For a period of 10 years after cessation of relationship with the client
Maintain records of all transactions	For a period of 10 years after the date of transaction

Appendix G - Interaction with partner agencies

Month	Institute/Academy	Interaction
April 2009	CBI Academy, Ghaziabad	AML Training for Inspectors of CBI
May 2009	National Academy of Direct Taxes, Nagpur	AML Seminar for Joint Commissioners of Income Tax
May 2009	CBI Academy, Ghaziabad	AML Seminar for senior officers of CBI
July 2009	CBI Academy, Ghaziabad	AML Seminar for DSPs and Inspectors of State Police
August 2009	CBI Academy, Ghaziabad	Training for CBI Inspectors working in Bank Fraud Investigation Teams
September 2009	National Academy of Direct Taxes, Nagpur	Seminar on Detection and Investigation of Financial Crimes for Assistant CITs, Deputy CITs, Joint CITs and Addl. CITs
September 2009	CBI Academy, Ghaziabad	Training for CBI Inspectors working in Bank Fraud Investigation Teams
January 2010	National Academy of Customs, Excise & Narcotics, Faridabad	AML Training Seminar for Deputy Commissioners and Joint Commissioners of Customs & Excise
January 2010	Narcotics Control Bureau, Chandigarh Zone	AML Seminar at Conference of Zonal Directors of NCB
February 2010	National Academy of Customs, Excise & Narcotics, Faridabad	AML Training Course for Deputy Commissioner, Joint Commissioners and Additional Commissioners of Customs & Excise
March 2010	National Academy of Customs, Excise & Narcotics, Faridabad	AML Training for IRS probationers of CBEC and CBDT

Appendix H Important FATF recommendations pertaining to Financial Intelligence Units

Recommendation 5 (Customer Due Diligence)

Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.

Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:

- establishing business relations;
- carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII;
- there is a suspicion of money laundering or terrorist financing; or
- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

Essential criteria

5.1 Financial institutions should not be permitted to keep anonymous accounts or accounts in fictitious names. Where numbered accounts exist, financial institutions should be required to maintain them in such a way that full compliance can be achieved with the FATF Recommendations. For example, the financial institution should properly identify the customer in accordance with these criteria, and the customer identification records should be available to the AML/CFT compliance officer, other appropriate staff and competent authorities.

When CDD is required

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

a) establishing business relations;

b) carrying out occasional transactions above the applicable designated threshold (USD/€ 15,000). This also includes situations where the transaction is carried out in a single operation or in several operations that appear to be linked;

c) carrying out occasional transactions that are wire transfers in the circumstances covered by the Interpretative Note to SR VII;

d) there is a suspicion of money laundering or terrorist financing, regardless of any exemptions or thresholds that are referred to elsewhere under the FATF Recommendations; or

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

Required CDD measures

5.3 Financial institutions should be required to identify the customer (whether permanent or occasional, and whether natural or legal persons or legal arrangements) and verify that customer‘s identity using reliable, independent source documents, data or information (identification data).

5.4 For customers that are legal persons or legal arrangements, the financial institution should be required to:

(a) verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person; and

(b) verify the legal status of the legal person or legal arrangement, e.g. by obtaining proof of incorporation or similar evidence of establishment or existence, and obtain information concerning the customer‘s name, the names of trustees (for trusts), legal form, address, directors (for legal persons), and provisions regulating the power to bind the legal person or arrangement.

5.5 Financial institutions should be required to identify the beneficial owner, and take reasonable measures to verify the identity of the beneficial owner10 using relevant information or data obtained from a reliable source such that the financial institution is satisfied that it knows who the beneficial owner is.

5.5.1 For all customers, the financial institution should determine whether the customer is acting on behalf of another person, and should then take reasonable steps to obtain sufficient identification data to verify the identity of that other person.

5.5.2 For customers that are legal persons or legal arrangements, the financial institution should be required to take reasonable measures to:

(a) understand the ownership and control structure of the customer;

(b) determine who are the natural persons that ultimately own or control the customer.

This includes those persons who exercise ultimate effective control over a legal person or arrangement

Examples of the types of measures that would be normally needed to satisfactorily perform this function include:

- For companies - identifying the natural persons with a controlling interest and the natural persons who comprise the mind and management of company.
- For trusts - identifying the settlor, the trustee or person exercising effective control over the trust, and the beneficiaries.

5.6 Financial institutions should be required to obtain information on the purpose and intended nature of the business relationship.

5.7 Financial institutions should be required to conduct ongoing due diligence on the business relationship.

5.7.1 Ongoing due diligence should include scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, and where necessary, the source of funds.

5.7.2 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 or business relationships.

Risk

5.8 Financial institutions should be required to perform enhanced due diligence for higher risk categories of customer, business relationship or transaction.

Examples of higher risk categories (which are derived from the Basel CDD Paper) may include11

a) Non-resident customers,
b) Private banking,
c) Legal persons or arrangements such as trusts that are personal assets holding vehicles,
d) Companies that have nominee shareholders or shares in bearer form.

Types of enhanced due diligence measures may include those set out in Recommendation 6.

5.9 Where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures. The general rule is that customers must be subject to the full range of CDD measures, including the requirement to identify the beneficial owner. Nevertheless there are circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the customer and the beneficial owner of a customer is publicly available, or where adequate checks and controls exist elsewhere in national systems. In such circumstances it could be reasonable for a country to allow its financial institutions to apply simplified or reduced CDD measures when identifying and verifying the identity of the customer and the beneficial owner.

Examples of customers, transactions or products where the risk may be lower could include:

a) Financial institutions – provided that they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are supervised for compliance with those requirements.

b) Public companies that are subject to regulatory disclosure requirements. This refers to companies that are listed on a stock exchange or similar situations.

c) Government administrations or enterprises.

d) Life insurance policies where the annual premium is no more than USD/€1000 or a single premium of no more than USD/€2500.

e) Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral.

f) A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

g) Beneficial owners of pooled accounts held by DNFBP provided that they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are subject to effective systems for monitoring and ensuring compliance with those requirements.

5.10 Where financial institutions are permitted to apply simplified or reduced CDD measures to customers resident in another country, this should be limited to countries that the original country is satisfied are in compliance with and have effectively implemented the FATF Recommendations.

5.11 Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

5.12 Where financial institutions are permitted to determine the extent of the CDD measures on a risk sensitive basis, this should be consistent with guidelines issued by the competent authorities.

Timing of verification

5.13 Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers.

5.14 Countries may permit financial institutions to complete the verification of the identity of the customer and beneficial owner following the establishment of the business relationship, provided that:

(a) This occurs as soon as reasonably practicable.
(b) This is essential not to interrupt the normal conduct of business.
(c) The money laundering risks are effectively managed.

Examples of situations where it may be essential not to interrupt the normal conduct of business are:

- Non face-to-face business.
- Securities transactions. In the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed.
- Life insurance business – in relation to identification and verification of the beneficiary under the policy. This may take place after the business relationship with the policyholder is established, but in all such cases, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

5.14.1 Where a customer is permitted to utilise the business relationship prior to verification, financial institutions should be required to adopt risk management procedures concerning the conditions under which this may occur. 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 of expected norms for that type of relationship.

Failure to satisfactorily complete CDD

5.15 Where the financial institution is unable to comply with Criteria 5.3 to 5.6 above:

a) it should not be permitted to open the account, commence business relations or perform the transaction;

b) it should consider making a suspicious transaction report.

5.16 Where the financial institution has already commenced the business relationship e.g. when Criteria 5.2(e), 5.14 or 5.17 apply, and the financial institution is unable to comply with Criteria 5.3 to 5.5 above it should be required to terminate the business relationship and to consider making a suspicious transaction report.

Existing customers

5.17 Financial institutions should be required to apply CDD requirements to existing customers on the basis of materiality and risk and to conduct due diligence on such existing relationships at appropriate times.

For financial institutions engaged in banking business (and for other financial institutions where relevant) - examples of when it may otherwise be an appropriate time to do so is when: (a) a transaction of significance takes place, (b) customer documentation standards change substantially, (c) there is a material change in the way that the account is operated, (d) the institution becomes ware that it lacks sufficient information about an existing customer.

5.18 Financial institutions should be required to perform CDD measures on existing customers if they are customers to whom Criterion 5.1 applies.

Recommendation 10 (Record keeping)

Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or 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 keep records on the identification data obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended.

The identification data and transaction records should be available to domestic competent authorities upon appropriate authority.

Essential criteria

10.1 Financial institutions should be required to maintain all necessary records on transactions, both domestic and international, for at least five years following completion of the transaction (or longer if requested by a competent authority in specific cases and upon proper authority). This requirement applies regardless of whether the account or business relationship is ongoing or has been terminated.

Examples of the necessary components of transaction records include: customer‘s (and beneficiary‘s) name, address (or other identifying information normally recorded by the intermediary), the nature and date of the transaction, the type and amount of currency involved, and the type and identifying number of any account involved in the transaction.

10.1.1 Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

10.2 Financial institutions should be required to maintain records of the identification data, account files and business correspondence for at least five years following the termination of an account or business relationship (or longer if requested by a competent authority in specific cases upon proper authority).

10.3 Financial institutions should be required to ensure that all customer and transaction records and information are available on a timely basis to domestic competent authorities upon appropriate authority.

Recommendation 13 (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, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

Essential criteria

13.1 A financial institution should be required by law or regulation to report to the FIU (a suspicious transaction report – STR) when it suspects or has reasonable grounds to suspect26 that funds are the proceeds of a criminal activity. At a minimum, the obligation to make a STR should apply to funds that are the proceeds of all offences that are required to be included as predicate offences under Recommendation 1. This requirement should be a direct mandatory obligation, and any indirect or implicit obligation to report suspicious transactions, whether by reason of possible prosecution for a ML offence or otherwise (so called ? indirect reporting), is not acceptable.

13.2 The obligation to make a STR also applies to funds where there are reasonable grounds to suspect or they are suspected to be linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism.

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

13.4 The requirement to report suspicious transactions should apply regardless of whether they are thought, among other things, to involve tax matters.

Additional elements

13.5 Are financial institutions required to report to the FIU when they suspect or have reasonable grounds to suspect that funds are the proceeds of all criminal acts that would constitute a predicate offence for money laundering domestically?

Recommendation 26 (Establishing an FIU)

Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

Essential criteria

26.1 Countries should establish an FIU that serves as a national centre for receiving (and if permitted, requesting), analysing, and disseminating disclosures of STR and other relevant information concerning suspected ML or FT activities. The FIU can be established either as an independent governmental authority or within an existing authority or authorities.

26.2 The FIU or another competent authority should provide financial institutions and other reporting parties with guidance regarding the manner of reporting, including the specification of reporting forms, and the procedures that should be followed when reporting.

26.3 The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

26.4 The FIU, either directly or through another competent authority, should be authorised to obtain from reporting parties additional information needed to properly undertake its functions.

26.5 The FIU should be authorised to disseminate financial information to domestic authorities for investigation or action when there are grounds to suspect ML or FT.

26.6 The FIU should have sufficient operational independence and autonomy to ensure that it is free from undue influence or interference.

26.7 Information held by the FIU should be securely protected and disseminated only in accordance with the law.

26.8 The FIU should publicly release periodic reports, and such reports should include statistics, typologies and trends as well as information regarding its activities.

26.9 Where a country has created an FIU, it should consider applying for membership in the Egmont Group.

26.10 Countries should have regard to the Egmont Group Statement of Purpose and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases (these documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIU).

Recommendation 40 (International Cooperation)

Countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to both money laundering and the underlying predicate offences. Exchanges should be permitted without unduly restrictive conditions. In particular:

a) Competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters.

b) Countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide co-operation.

c) Competent authorities should be able to conduct inquiries; and where possible, investigations; on behalf of foreign counterparts.

Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts. Co-operation with foreign authorities other than counterparts could occur directly or indirectly. When uncertain about the appropriate avenue to follow, competent authorities should first contact their foreign counterparts for assistance.

Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection.

Essential criteria

40.1 Countries should ensure that their competent authorities are able to provide the widest range of international cooperation to their foreign counterparts.

40.1.1 Countries should be able to provide such assistance in a rapid, constructive and effective manner.

40.2 There should be clear and effective gateways, mechanisms or channels that will facilitate and allow for prompt and constructive exchanges of information directly between counterparts.

Examples of gateways, mechanisms or channels used in international cooperation and exchanges of information (other than MLA or extradition) include laws allowing exchanges of information on a reciprocal basis; bilateral or multilateral agreements or arrangements such as Memorandum of Understanding (MoU); and exchanges through appropriate international or regional organisations or bodies such as Interpol or the Egmont Group of FIUs.

40.3 Such exchanges of information should be possible: (a) both spontaneously and upon request, and (b) in relation to both money laundering and the underlying predicate offences.

40.4 Countries should ensure that all their competent authorities are authorised to conduct inquiries on behalf of foreign counterparts.

40.4.1 In particular, countries should ensure that their FIU is authorised to make the following types of inquiries on behalf of foreign counterparts: (a) searching its own databases, including with respect to information related to suspicious transaction reports; (b) searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases and commercially available databases.

40.5 Countries should ensure that their law enforcement authorities are authorised to conduct investigations on behalf of foreign counterparts; other competent authorities should be authorised to conduct investigations on behalf of foreign counterparts, where permitted by domestic law.

40.6 Exchanges of information should not be made subject to disproportionate or unduly restrictive conditions.

40.7 Requests for cooperation should not be refused on the sole ground that the request is also considered to involve fiscal matters.

40.8 Requests for cooperation should not be refused on the grounds of laws that impose secrecy or confidentiality requirements on financial institutions or DNFBP (except where the relevant information that is sought is held in circumstances where legal professional privilege or legal professional secrecy applies).

40.9 Countries should establish controls and safeguards to ensure that information received by competent authorities is used only in an authorised manner. These controls and safeguards should be consistent with national provisions on privacy and data protection.

Additional elements

40.10 Are mechanisms in place to permit a prompt and constructive exchange of information with non-counterparts? Does it take place directly or indirectly?

40.10.1Does the requesting authority as a matter of practice disclose to the requested authority the purpose of the request and on whose behalf the request is made?

40.11 Can the FIU obtain from other competent authorities or other persons relevant information requested by a foreign counterpart FIU?

Special Recommendation IV. Reporting suspicious transactions related to terrorism

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organisations, they should be required to report promptly their suspicions to the competent authorities.

Essential criteria

IV.1 A financial institution should be required by law or regulation to report to the FIU (a suspicious transaction report – STR) when it suspects or has reasonable grounds to suspect that funds are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism. This requirement should be a direct mandatory obligation, and any indirect or implicit obligation to report suspicious transactions, whether by reason of possible prosecution for a FT offence or otherwise (so called ? indirect reporting?), is not acceptable.

IV.2 Countries should ensure that Criteria 13.3 – 13.4 (in R.13) also apply in relation to the obligations under SR IV.

Special Recommendation V. International Co-operation

Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts

Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals and terrorist organisations.

Essential criteria

V.1 Countries should ensure that Criteria 36.1 – 36.7 (in R.36) also apply to the obligations under SR.V53.

V.2 Countries should ensure that Criteria 37.1 &37.2 (in R.37) also apply to the obligations under SR.V.

V.3 Countries should ensure that Criteria 38.1 – 38.5 (in R.38) also apply to the obligations under SR.V.

V.4 Countries should ensure that Criteria 39.1 – 39.4 (in R.39) also apply to extradition proceedings related to terrorist acts and FT.

V.5 Countries should ensure that Criteria 40.1 – 40.9 (in R.40) also apply to the obligations under SR.V.

Additional elements

V.6 Does the additional element 36.8 (in R.36) apply in relation to the obligations under SR.V?

V.7 Does additional element 38.6 (in R.38) apply in relation to the obligations under SR.V?

V.8 Does the additional element 39.5 (in R.39) apply extradition proceedings related to terrorist acts or FT?

V.9 Do additional elements 40.10 – 40.11 (in R.40) apply in relation to the obligations under SR.V?

Appendix I - Outreach Programmes conducted during the year 2009-10

April 2009	• Workshop for ANMI (Association of NSE Members of India) for DPs and Brokers at Delhi and Mumbai • Interaction with AML Team of HSBC at Mumbai • Workshop for SBI at Nagaland and Guwahati • Seminar for CAs and Tax Professionals at Delhi
May 2009	• Seminar for Institute of Chartered Accountants of India at Pune for their member Chartered Accountants • Workshop for officers PSU Banks, Private Sector Banks, RRBs, NABARD of the North East region at Itanagar, for Dena Bank at Mumbai, and for Punjab & Sind Bank at Chandigarh • Regional Supervision Seminar for inspection staff of NABARD at Trivandrum • Workshop for POs and AML teams of Associate Banks of SBI at Delhi
Jun 2009	• Interaction with top management of State Bank of Hyderabad at Hyderabad • Seminar for SBI at Dehradun and Shimla and for PNB at Delhi • Interactions with AML teams of Oriental Bank of Commerce, Punjab National Bank and Punjab & Sind Bank at Delhi • Seminar for senior officers of RBI (DGMs) at Chennai • Workshop for front office managers and AML Team of Citibank at Chennai • Workshop for NABARD Inspection staff at Kolkata
July 2009	• Seminar and training for transaction monitoring for SBI & its Associate Banks at Jaipur • Seminar for SBI at Chennai, for Dena Bank at Ahmedabad, for Kotak Mahindra Bank at Kolkata, for ING Vysya Bank at Kolkata • Seminar with RBI for Officers of banks in North East region at Guwahati and for RBI officers of Mumbai region at Mumbai • Seminar for inspection staff of NABARD at Lucknow • Seminar for its member Company Secretaries at Kolkata • Students conference for Institute of Company Secretaries of India for students of the Institute at Kolkata • Training for Cooperative Banks at Bhopal • Seminar for AML Team of ICICI Bank at Mumbai
August 2009	• Workshop for Officers of Banking Supervision Department of RBI at Delhi • Workshops with NABARD for Principal Officers of RRBs and DCBs at Lucknow and Bhopal • Workshop for Western Union Money Transfer and their agents at Mumbai • Workshop for Oriental Bank of Commerce at Bangalore
September 2009	• Workshop for J&K Bank at Srinagar • Interactions with top management and AML Teams of Indian Overseas Bank and Indian Bank at Chennai • Interaction with top management and AML Team Computer Age Management Services Pvt. Ltd. (CAMS) at Chennai • Seminar for ING Vysya Bank at Delhi • Workshops for RRBs at Kolar, Mysore, Mandya and Bangalore in Karnataka • Interaction with Principal Officer and AML Team of Standard Chartered Bank at Gurgaon
October 2009	• 'Train the Trainers' program on AML/CFT capacity building for officers from faculty of training institutes of reporting entities at New Delhi • Seminar for Corporation Bank at Delhi, and Karnataka Bank and Syndicate Bank at Bangalore • Interaction with AML Team of HDFC Bank at Mumbai and with AML Team of HSBC at Delhi
November 2009	• Workshop for and interaction with AML Team of SBI at Jaipur • Workshop for Central Bank of India at Mumbai • Interaction with AML Team and top management of Central Bank of India and Union Bank of India at Mumbai • Workshop for business heads and AML Team of Saraswat Cooperative Bank at Mumbai • Workshop for Casinos at Goa • Workshop for capital market intermediaries at Mumbai • Seminar for Regional Director and senior management of NABARD at Lucknow
December 2009	• Workshop for Canara Bank at Delhi, for Citibank at Pune and for Punjab & Sind Bank at NOIDA • Workshop for insurance companies at National Insurance Academy, Pune • Workshop for AGMs and DGMs of RBI's Banking Supervision Department at Chennai

January 2010	• Seminar for SBI at Bhopal and Vishakhapatnam, for Union Bank of India at Mumbai, for ING Vysya Bank of Rajasthan region at Jaipur, and for Associate Banks of SBI at Jaipur • Workshop for Housing Finance Companies and NHB at Mumbai
February 2010	• Workshop for Bank of Baroda at Ahmedabad, for UCO Bank at Patna and Delhi, Allahabad Bank at Patna, Karnataka Bank at Delhi, Corporation Bank at Chandigarh, and Union Bank of India and Central Bank of India at Lucknow • Workshop for regional officers of housing finance companies at Chennai • Interaction with Bank of Rajasthan at Jaipur and Jodhpur, and PNB at Jaipur • Workshop for Paul Merchants Ltd. (Agent of Western Union Money Transfer) at Chandigarh
March 2010	• Workshop for Citibank and State Bank of Indore at Indore • Workshop for DB International Brokers at Delhi

Glossary

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
CBS	Core Banking Solution
CCR	Counterfeit Currency Report
CEIB	Central Economic Intelligence Bureau
CFT	Combating Financing of Terrorism
CIT	Commissioner of Income Tax
CTED	Counter Terrorism Executive Directorate
CTR	Cash Transaction Report
DNFBP	Designated Non-Financial Businesses and Professions
ED	Enforcement Directorate
EOI	Expression of Interest
ESW	Egmont Secure Web
E&Y	Ernst & Young
FATF	Financial Action Task Force
FEMA	The Foreign Exchange Management Act, 1999
FICN	Fake Indian Currency Notes
FINnet	Financial Intelligence Network
FIU	Financial Intelligence Unit
FIU-IND	Financial Intelligence Unit, India
FSRB	FATF Style Regional Bodies
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
IT	Information Technology
JWG	Joint Working Group
LEA	Law Enforcement Agency
KYC	Know Your Customer
MEQ	Mutual Evaluation Questionnaire
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
OpWG	Operational Working Group
PAN	Permanent Account Number
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 Council
RFP	Request For Proposal

RPU	Report Preparation Utility
RRB	Regional Rural Bank
SEBI	Securities and Exchange Board of India
SI	System Integrator
STR	Suspicious Transaction Report
TF	Terrorist Financing
UAPA	The Unlawful Activities (Prevention) Act, 1967
UCB	Urban Co-operative Bank
UNSCR	United Nations Security Council Resolution
XML	Extensible Markup Language