Annual Report 2012-13

Financial Intelligence Unit-India

Ministry of Finance, Government of India

सत्यमेव जयते

Annual Report
2012-13

Department of Revenue
Ministry of Finance, Government of India

Director's Report

Director's Report

The year 2012-13 has been a water-shed in the history of FIU-IND. In October 2012, the FINGate module of Project FINnet was commissioned enabling the reporting entities to file their reports online. This was a paradigm shift from the old regime when the reports would be filed on paper or through CDs. Project FINnet was fully commissioned in March 2013 enabling FIU-IND to completely automate its receipt, analysis and dissemination functions. FIU-IND has embarked on an ambitious programme to register the reporting entities as well as the law enforcement authorities on the FINnet.

The year also saw important changes in the legislative framework for FIU's functioning. The PML Act was amended effective 15 February 2013, bringing more reporting entities under its purview (e.g. DNFB's, Stock Exchanges, Commodity market entities, India Post, Sub-registrars of property etc.); removing monetary threshold for the predicate offences; strengthening of KYC, record-keeping and reporting obligations; broadening the range of sanctions that could be imposed on the reporting entities and protecting the reporting entities from civil or criminal liability in discharge of their obligations under the PML Act.

The year also saw overall improvement in the quantity and quality of the reports received. Over 31,700 STRs were received, together with 5,707 CCRs and nearly 89 lakh CTRs, notwithstanding the challenges posed by the switchover to the new report filing procedure in the FINGate. The STRs disseminated included 395 category 'A' STRs.

Hon. Finance Minister visited FIU-IND premises in August 2012 and shared his strategic vision for the FIU, which will guide us in the future. Pursuant to his visit, a Virtual Office was set up in January 2013 to monitor follow-up action on FIU's STRs.

FIU-IND continued with its active participation in international cooperation on AML/CFT. Apart from proactive information exchange, FIU-IND made significant contribution to the Egmont Group activities, by participating in the Charter Review exercise and representing Asia region on the Egmont Committee. FIU-IND also signed MOUs with four countries for exchange of information and provided technical assistance to FIU-Bhutan.

As part of its outreach programme, FIU-IND participated in 38 workshops/seminars for the reporting entities covering more than 2,800 participants. In addition, 28 review meetings were held with the reporting entities covering 1,471 officers. In enforcement of compliance, 208 advisories were issued and monetary penalty was imposed on one reporting entity.

I take this opportunity to compliment the officer and staff of FIU-IND for their dedicated work, which has brought FIU-IND appreciation from all quarters.

(P K Tiwari)
Director
Financial Intelligence Unit-India

Table of Contents

Performance at a Glance : 2012-13

Information received

- **8.8 million** Cash Transaction Reports (CTRs); **99.95%** in electronic form
- **31,729** Suspicious Transaction Reports (STRs)
- **3,62,371** Counterfeit Currency Reports (CCRs)

Information analysed & disseminated

- **13,407** STRs analysed
- **10,466** STRs disseminated

Collaboration with domestic Law Enforcement and Intelligence Agencies

- Received **549** requests for information
- Provided information in **534** cases

Internal cooperation & exchange of information

- **73** requests received from foreign FIUs
- **69** requests sent to foreign FIUs

Spreading awareness about money laundering and terrorism financing

- Contributed in **31** seminars and training workshops covering **2,077** participants
- Organized the 'Train the Trainer' programme for AML/CFT capacity building with **63** participants.
- Organized a workshop on "The Risk Based Approach and the National ML/ TF Risk Assessment" for **60** representatives of reporting entities and law enforcement agencies.

Improving compliance with the PMLA

- **21** review meetings held with Principal Officers

Strengthening legislative and regulatory framework

- Worked with Department of Revenue on drafting the amendments to Prevention of Money Laundering Act, 2002 and PML (Maintenance of Records) Rules, 2005.
- Participated in proceedings of the AML Steering Committee for evolving Risk Based Approach and framing of the National ML/ TF Risk Assessment.

Strengthening IT infrastructure

- Project FINnet commissioned. Maintenance phase commenced.
- Successful end-to-end flow of information from reporting entities to FIU to law enforcement agencies implemented.

Chapter 1

Financial Intelligence Unit – India

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

The new Charter of Egmont group has adopted the definition of a Financial Intelligence Unit (FIU) as stated within the text of the FATF Recommendation and Interpretative Note on Financial Intelligence Units (Recommendation 29). It states -

"Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of:

(a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis.

The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly".

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

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

Financial Intelligence Unit-India (FIU-IND) was established by the Government of India vide Office Memorandum dated 18th November, 2004 for coordinating and strengthening collection and sharing of financial intelligence through an effective national, regional and global network to combat money

laundering and related crimes. It is an independent body reporting to the Economic Intelligence Council (EIC) headed by the Finance Minister. For administrative purposes, FIU-IND is under the control of Department of Revenue, Ministry of Finance.

FIU-IND is established as an administrative FIU i.e, as an independent government body, that receives, analyses and disseminates STRs to the notified law enforcement or investigation agencies.

FIU-IND does not investigate cases.

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

As prescribed under the Prevention of Money Laundering Act (PMLA) and the rules framed thereunder, FIU-IND receives reports on cash transactions, suspicious transactions, counterfeit currency transactions and funds received by non-profit organisations. These reports are filed by the reporting entities i.e. banks, financial institutions and capital market intermediaries. FIU-IND analyses the reports received and shares with agencies specified in or notified under Section 66 of PMLA. Two new reports have been introduced with effect from 15th February 2013, one relating to cross border transactions and other on immovable properties registered by Sub-registrar or Registrar. New reporting entities were brought under the PMLA through an amendment in February 2013 and include designated non-financial businesses and professions e.g. India Post, Stock Exchange and the entities regulated by Pension Fund Regulatory and Development Authority (PFRDA).

Reports required to be filed under PMLA

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

FIU-IND maintains a database of the financial transactions reported to it. The results of the analysis of the information received are shared with enforcement and intelligence agencies voluntarily and on request. FIU-IND also monitors and identifies strategic and key money laundering trends, typologies and developments based on the analysis of its databases.

Mission, Vision and Strategic Goals 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.

Mission Statement

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

Organization Vision

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

FIU-IND, in order to achieve its mission, 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 to combat ML & FT

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

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

This Report reviews the performance of FIU-IND during the year 2012-13 under the above mentioned thrust areas.

Action Plan for 2012-13

Overall, the key result areas (KRAs) showed better results over the previous year, as shown in the last column of Table- 1.

Table 1: Performance in Key Result Areas (2012-13)

Sl. No.	Major Objective	Actions required to achieve the objective	Success indicators for monitoring/ achieving the objective	Targets for 2012-13	Result
1.	Receiving reports in electronic format	i) Assisting reporting entities by providing enabling tools ii) Enhanced outreach programmes	Majority of reports are received in electronic format	More than 99.8% reports in electronic format	Percentage of reports received was 99.96 %.
2.	Improving quality of analysis	i) Access to LEA/IA databases ii) Increase in analytical staff iii) Detailed analysis of category 'A' STRs	Better quality of dissemination notes	Better quality of analysis with value addition in category 'A' STRs	395 category 'A' STRs, were disseminated to LEAs/IAs.
3.	Improving compliance with reporting obligations under PMLA by the reporting entities	i) Monitoring implementation of AML software by the reporting entities ii) Regular review meetings with reporting entities	Submission of STRs by new entities	- At least 20 review meetings with reporting entities	28 review meetings with reporting entities were held.
4.	Improving information exchange with domestic IAs/LEAs	i) Periodical meetings with domestic IAs/LEAs ii) Training to LEA/IA staff	Increase in information exchange with IAs/LEAs	At least 200 exchanges with domestic agencies	549 requests received from domestic agencies.
5.	Enhanced international cooperation	i) Substantial increase in exchange of information with foreign FIUs ii) Negotiation of MOUs with more FIUs	Number of cases in which information is exchanged	At least 125 exchanges with foreign FIUs	More than 200 exchanges with foreign FIUs.
6.	Project FINnet	i) Implementation of online gateway to receive reports ii) Implementation of analysis and dissemination system	Online receipt of reports from reporting entities	Operationalization of online gateway.	The project was commissioned in March 2013.

Chapter 2

Legal framework

Prevention of Money Laundering Act, 2002

The Prevention of Money Laundering Act, 2002 (PMLA), India's legislation for combating money laundering, was enacted in 2002 and brought into force on 1st July 2005. It provides for receipt and dissemination of reports relating to money laundering and for attachment, seizure and confiscation of property obtained or derived, directly or indirectly, from or involved in money laundering. The PMLA was enacted to implement the resolution and declaration made under the Political Declaration and Global Programme of Action against Money Laundering adopted by the General Assembly of the United Nations in 1998. The Unlawful Activities (Prevention) Act, 1967 (UAPA) is the legislation to combat terrorism and financing of terrorism.

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 including its concealment, possession, acquisition or use and projecting or claiming 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 up to seven years as well as a fine. 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 two parts of the schedule – Part A incorporates crimes against the

state, terrorism, drug related crimes, and other crimes against property & individuals, economic crimes, etc., and Part C includes cross-border crimes. The Schedule includes 156 offences under 28 different laws. A list of predicate offences is at Appendix C.

PMLA incorporates two different sets of provisions – one set of provisions relating to maintenance and submission of information to FIU and the second set of provisions relating to investigations into cases of money laundering and powers of search, seizure, collection of evidence, prosecution, etc. The Director, FIU-IND is the relevant authority for the provisions relating to maintenance of records and filing of information. The Directorate of Enforcement is the authority for the provisions relating to search, seizure, confiscation of property, prosecution, etc.

A list of important Rules notified by the Central Government under PMLA is listed at Appendix D. A List of important circulars/ instructions on AML/CFT issued by the Regulators is at Appendix E.

Overview of PMLA

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

Amendments to PML Act

The PMLA 2002 has been amended first in 2005 and thereafter in 2009 to overcome some of the difficulties that were being faced in its enforcement and to increase the coverage of the Act. A comprehensive evaluation of the country's legislative and administrative framework for prevention of money laundering and countering financing of terror was made by the FATF in November/December, 2009. To align the Act further to the international standards, amendments were proposed by the Government through the introduction of Prevention of Money Laundering (Amendment) Bill, 2011. The Bill was examined by the Parliament's Standing Committee on Finance and after considering their recommendations, the revised Prevention of Money Laundering (Amendment) Bill, 2012 was passed by the two houses of Parliament in November/December

2012. It received the assent of the President on the 3rd January 2013. Upon notification the amendments came into effect from 15th February 2013. The salient features of some important amendments relevant to the working of FIU are discussed as under:

A. Definition of Offence of Money Laundering

The definition of the offence of Money laundering under section 3 has been expanded to include concealment, possession, acquisition and use of the proceeds of crime as criminal activities for money laundering in line with Article 6 of Palermo Convention.

B. Punishment for Money Laundering

Section 4 has been amended to provide for imposition of fine proportionate to the gravity of the offence which will be determined by the court. The limit of Rs.5 lakh has been deleted altogether. Further, an explanation has been inserted in Section 70 that the prosecution or conviction of any legal juridical person shall not be contingent on the prosecution or conviction of any individual.

C. Removing monetary threshold for investigating the offence of money laundering

To conform to the FATF standards, the offences in Part B of the schedule have been moved to Part A thereby removing the monetary threshold of Rupees 30 lakh.

D. Strengthening of KYC, record keeping and reporting obligations

Section 12 has been amended to clearly specify that a reporting entity shall maintain records of all transaction including transactions reported to FIU-IND, identify the beneficial owner of its clients, maintain records of identity of such beneficial owners and keep the information maintained, furnished or verified confidential.

E. Inclusion of additional financial sector entities under PMLA

Following financial sector entities have been brought under the ambit of PMLA:

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

b) Members of Commodity Exchanges (Commodity Brokers)

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

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

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

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

A new category of entities i.e. “person carrying on designated business or profession” has been created under Section 2(1)(sa) to cover the following :

a) Registrar or Sub-Registrar appointed under section 6 of the Registration Act, 1908 (16 of 1908),

b) Real estate agent,

c) Dealer in precious metals, precious stones and other high value goods and,

d) Person engaged in safekeeping and administration of cash and liquid securities on behalf of other persons.

The obligations under PMLA shall apply to the above persons after being notified by the Central Government, which has the power to notify any other person carrying out any other activities under this clause.

G. Measures for effective compliance

To strengthen the ability of FIU to ensure compliance, following amendments have been made:

a) Under section 12A powers have been given to the Director, FIU-IND to call for records of transaction or any additional information that may be required for the purpose of this Act.

b) A separate sub-section has been included to put an obligation on the reporting entity to maintain confidentiality of the request made under section 12 A.

c) Provision for appointment of special auditor for conducting audit in complex cases.

d) Provision for imposition of sanctions on designated director on the Board or any of the employees of the reporting entity which has failed to comply.

e) Expanding the range of sanctions to include warning in writing; directions to comply with specific instructions; direction to send reports on the measures a reporting entity is taking and imposing monetary penalty for failure to comply.

H. Protection from civil or criminal proceedings

Under section 14 protection has been given to Directors as well as employees of a reporting entity from criminal and civil liability for disclosure of information to FIU-IND.

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

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

a) Insurance Regulatory and Development Authority

b) Department of Posts

c) Forward Markets Commission

d) Pension Fund Regulatory and Development Authority

e) Registrar or Sub-Registrar appointed under section 6 of the Registration Act, 1908 (16 of 1908);

f) Registering authority empowered to register motor vehicles under Chapter IV of the Motor Vehicles Act, 1988 (59 of 1988)

g) Recognised stock exchange referred to in clause (f) of section 2 of the Securities Contracts (Regulation) Act, 1956 (42 of 1956);

h) The Institute of Chartered Accounts of India (ICAI)

i) The Institute of Cost and Works Accountants of India (ICWAI)

j) The Institute of Company Secretaries of India (ICSI)

Besides, several other amendments relating to attachment and freezing of property, making confiscation independent of conviction, procedure of confiscation, burden of proof, committing of cases to Special Court and appeal against the order of Appellate Tribunal to lie in the Supreme Court have also been made in the PMLA.

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 Unlawful Activities (Prevention) Amendment Bill, 2011 was introduced in Parliament in December 2011. The Bill was passed by both houses of Parliament in November/December 2012 and notified with effect from 1st February,2013. The Bill amends the Unlawful Activities (Prevention) Act, 1967 to make it more effective in preventing unlawful activities, and meet commitments made to the Financial Action Task Force. The salient features of amendment made in the Act are listed below:

(1) Increase the period of declaration of an association as unlawful from two years to five years as specified under section 6;

(2) Amendment in Section 15 of the principal act with the purpose of enlarging the ambit of 'terrorist act' by incorporating the 'economic security' of the country and to protect the monetary stability of India by way of production or smuggling or circulation of high quality counterfeit Indian paper currency, coin or of any other material. The international/intergovernmental organizations have been covered explicitly;

(3) To bring the cohesiveness in the legal framework, the provision of section 16A is proposed to be brought as clause (d) after clause (c) of the section and the existing 16A is being deleted;

(4) Amendments made to explicitly criminalize high quality counterfeiting. All the nine Treaties annexed to the

International Convention for the Suppression of the Financing of Terrorism (CFT) specifying various types of terrorist acts which constitute an offence are now to be listed in Second Schedule to this Act;

(5) Enlarging the scope of Section 17 of the Act relating to punishment for raising funds for terrorist act and include within its scope, raising of funds, both from legitimate or illegitimate sources, by a terrorist organization or by terrorist gang or by an individual terrorist;

(6) Insert new sections 22A, 22B and 22C in the Act to include within its scope, offences by companies societies or trusts and provide punishment therefor;

(7) Insert a new section 24 in the Act so as to enlarge the scope of proceeds of terrorism to include therein any property intended to be used for terrorism; and

(8) Insert sub-sections (3) to (5) in section 33 of the aforesaid Act to confer power upon the court by order to provide–

(i) for attachment or forfeiture of property equivalent to the counterfeit Indian currency involved in the offence, including the face value of such currency which are not defined to be of high quality but are part of the common seizure along with the high quality counterfeit Indian currency;

(ii) for attachment or forfeiture of property equivalent to or the value of the proceeds of terrorism involved in the offence; and

(iii) for confiscation of movable or immovable property on the basis of the material evidence where the trial cannot be concluded on account of the death of the accused or the accused being declared as a proclaimed offender or any other reason.

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.

Section 17 of the amended UAPA reads as under:

"Whoever, in India or in a foreign country, directly or indirectly, raises or provides funds or collects funds, whether from a legitimate or illegitimate source, from any person or persons or attempts to provide to, or raises or collects funds for any person or persons, knowing that such funds are likely to be used, in full or in part by such person or persons or by a terrorist organisation or by a terrorist gang or by an individual terrorist 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:

***"Offence of raising fund for a terrorist organization.**- (1) 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.*

Explanation.—For the purposes of this sub-section, a reference to provide money or other property includes—

(a) of its being given, lent or otherwise made available, whether or not for consideration; or

(b) raising, collecting or providing funds through production or smuggling or circulation of high quality counterfeit Indian currency

(2) 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 51A of UAPA allows the Government to freeze, seize or attach funds held by the individuals or entities engaged in terrorism. 36 entities are listed as banned organizations by Ministry of Home Affairs and together with other entities covered under UNSCR 1267 and 1373 they are declared as terrorist organizations under UAPA.

PMLA and FIU-IND

Sections 12 of PMLA requires every reporting entity including banking company, financial institution and intermediary and designated non-financial businesses as and professions to furnish information of prescribed transactions to the Director, FIU-IND and to verify the identity of all its clients in the manner prescribed. The reporting entities are also required to maintain and preserve records of transactions and records of identity of clients for a period specified in the Act.

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***.

The power of the Director to call for information from the reporting entities has been provided in section 12A. This empowers the Director to call for additional information from reporting entity apart from information furnished under section 12(1). Section 13 of PMLA empowers Director, FIU-IND to enquire into cases of suspected failure of compliance with the provisions of PMLA and impose sanctions including monetary penalty on reporting entity or its designated director or any of its employees which shall not be less than ten thousand rupees and may extend to one lakh rupees for each failure to comply with PMLA. Where Director in course of inquiry finds a case complex, he may direct the reporting entity to get its records audited by an accountant. The expense of the audit shall be paid by the Government. The other sanctions provided in section 13 include issue of warning in writing to the reporting entity, direct the reporting entity or its director or any of its employees to comply with specific instructions or direct them to send reports on the measures it is taking.

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

Categorization of Reporting Entities after PMLA amendment

Banking Companies	Financial Institutions	Intermediaries	DNFBP
▪ Public sector banks ▪ Private Indian banks ▪ Private foreign banks ▪ Co-operative banks ▪ Regional rural banks	▪ Insurance companies ▪ Hire purchase companies ▪ Chit fund companies ▪ Housing finance institutions ▪ Non-banking financial companies ▪ Payment system operators* ▪ Authorized persons ▪ India Post	▪ Stock brokers ; Sub-brokers ▪ Share transfer agents ▪ Registrars to issue ▪ Merchant bankers ▪ Underwriters ▪ Portfolio managers ▪ Investment advisers ▪ Depositories and DPs ▪ Custodian of securities ▪ Foreign institutional investors ▪ Venture capital funds ▪ Mutual funds ▪ Intermediary regulated by FMC ▪ Intermediary regulated by PFRDA ▪ Recognized stock exchanges	▪ Casino ▪ Registrar or Sub-registrar ▪ Real Estate Agent ▪ Dealer in precious metals, precious stones and other high value goods ▪ Private Locker operators (Upon notification by the Central Govt.)

Note: The new reporting entities are indicated in italics.

Chapter 3

Receipt, Analysis and Dissemination of Information

The foundation of FIU-IND's work is receipt of the suspicious transaction reports and other prescribed reports from the reporting entities that are analysed and results of analysis are disseminated to the partner agencies as provided under section 66 of the PMLA, 2002. The intelligence inputs so shared may be used in the investigation of the predicate and other offences. The results of analysis of financial information received from the reporting entities in the form of various prescribed reports has proven to be of considerable value in the investigation of money laundering, terrorist financing and other crimes investigated by the law enforcement agencies.

FIU-IND's ambitious information technology system called 'FINnet' has been launched in October 2012. It enables the reporting entities to upload and furnish all their reports to FIU-IND online using its FINgate portal. The FinCore portal of the FINnet processes the reports received from the reporting entity and links all relevant reports available in the FIU databases using rules of identity and relationship resolution. A case so formed around a suspicious transaction report thus contains not only the information received from a particular reporting entity but all other relevant information/ reports that might have been furnished by other reporting entities. Thus a lot of value gets added to the information received from the reporting entities before the same is disseminated to the partner agencies for their consumption/ use.

The number of STRs received, analyzed and disseminated has shown increasing trend. Focussed attention on thrust areas ensured that there was consistent improvement in the quality of reporting.

Receipt of information

Section 12 of the PMLA and rules framed thereunder require the reporting entities to furnish to FIU-IND information relating to prescribed cash transactions, suspicious transactions, cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine, and transactions

involving receipts by non-profit organizations. As part of the IT modernization programme the existing formats of the reports have been converted into three reporting formats, namely, accounts based reporting format, transactions based reporting format, and reporting format for the CCRs.

Cash Transaction Reports

PMLA requires the reporting entities to furnish to FIU-IND information relating to-

- All cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency; and
- 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 for the month are to be furnished on a monthly basis by the 15th day of the succeeding month.

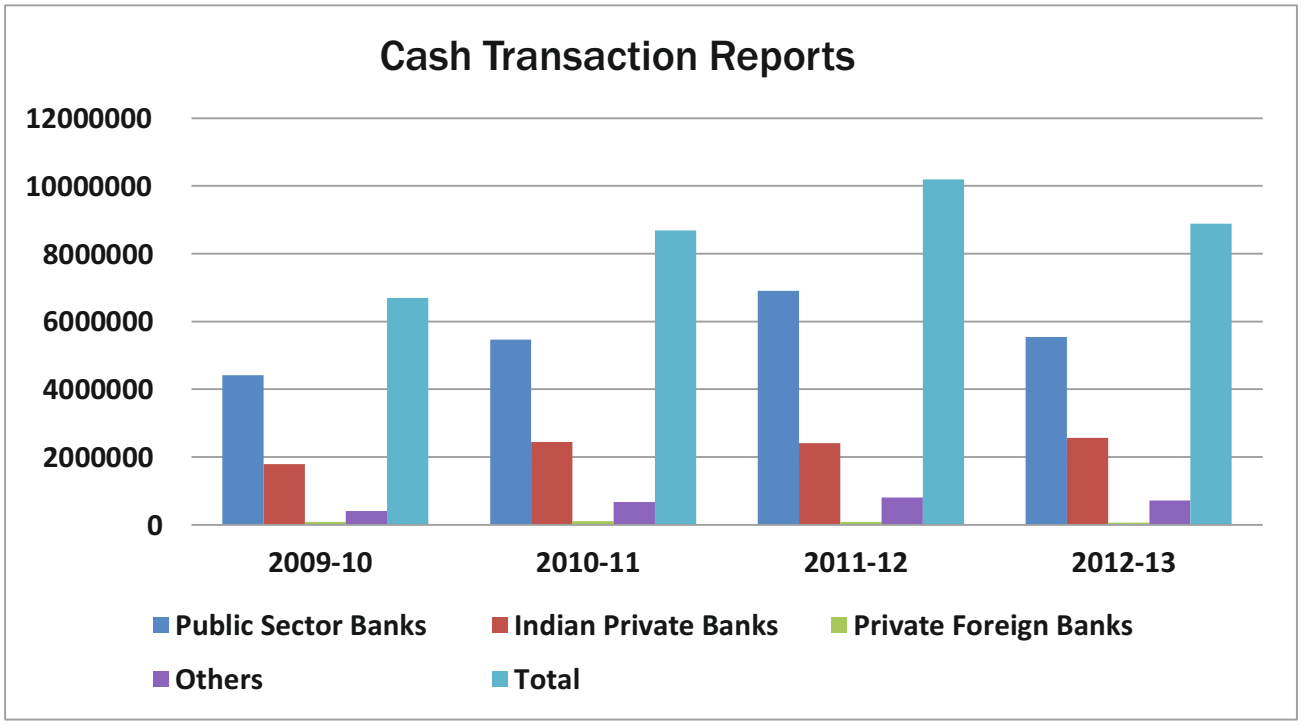
Trends in CTRs

- 8.8 million CTRs were reported in 2012-13 as compared to 10.1 million CTRs in the previous year.
- The decline in the number of CTRs has been noticed in respect of all types of banks except Indian private banks.
- The decline is most pronounced in case of public sector banks (from 6.9 million in 2011-12 to 5.5 million in 2012-13).
- All reports w.e.f. 20th October, 2012 have been filed online using the FINgate portal of FIU-IND.
- The decline in reports filed is largely due to the initial problems relating to understanding and adoption of new technology for filing online report (FINgate).

Majority of the CTRs received during the year continued to be from the Public Sector Banks. Efforts were made to ensure that the smaller banks such as district co-operative banks and regional rural banks do not face too much difficulty in adopting the new technology for filing of CTRs and other reports online. However, it appears that a number of banks, including large public and private sector banks faced initial problems with the new technology, which partially explains the decline in the number of CTRs for the first time since FIU-IND was established. FIU-IND is making all out efforts to train the key persons in the banks in filing of online reports. The reporting entities are encouraged to file the reports using digital signature so as to make the filing instantaneous. The number of CTRs received in previous four years is given below (Table 1).

Table 2 : Receipt of Cash Transaction Reports from the Banking Companies

Type of Bank	2009-10	2010-11	2011-12	2012-13
Public Sector Banks	44,13,849	54,63,252	69,03,096	55,41,408
Indian Private Banks	17,84,665	24,42,286	24,06,855	25,61,548
Private Foreign Banks	84,428	1,05,288	83,665	58,640
Co-operative Banks and others	4,11,462	6,76,281	8,04,646	7,20,622
Total	66,94,404	86,87,107	1,01,98,262	88,82,218



Suspicious Transaction Reports

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

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

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

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

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

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

Majority of the STRs received from the reporting entities fall in the sub-clause (b) and (c) of the definition of suspicious transaction given above.

Suspicious Transaction Reports (STRs) are required to be furnished by the principal officer of the reporting entity not later than seven working days on being satisfied that the transaction is suspicious.

A working group consisting of representatives of Banks, RBI, Indian Banks Association (IBA), and FIU-IND identified red flag indicators for generating alerts against transactions which could be suspect based on certain criteria. The guidance note was issued by the IBA for implementation by all banks. Similar working groups have been formed for identifying red flag indicators for Money Transfer Service Businesses and Card System Operators.

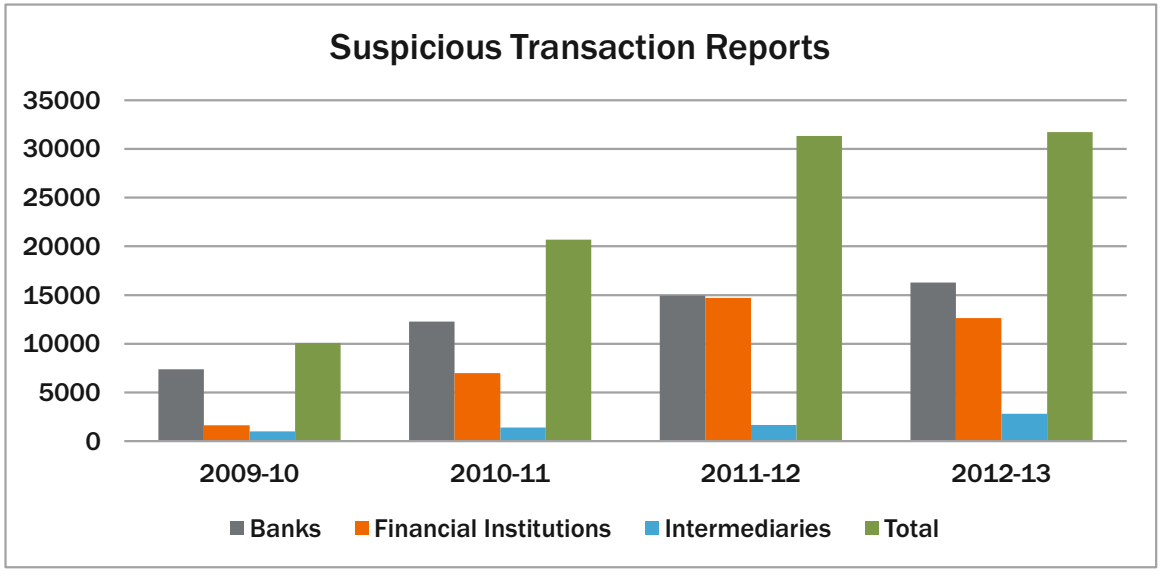
The "Train the Trainers" programme conducted once a year by FIU-IND has produced the desired cascading effect in spreading AML/CFT awareness across the reporting entities. The resource persons who were trained by FIU-IND in turn imparted training to a large number of employees in their respective organizations.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

Trends in STRs

- The number of STRs remained at the same level as 2011-12 (about 31,000 STRs).
- The STRs filed by the intermediaries registered a growth of 70% in 2012-13 over the preceding year.
- Amongst Financial Institutions, Money Transfer Service Agents filed maximum STRs.
- The lack of growth in STRs filed is largely due to the initial problems relating to understanding and adoption of new technology for filing online report (FINgate).

Table 3: Receipt of Suspicious Transaction Reports

Category	2009-10	2010-11	2011-12	2012-13
Banks	7,394	12,287	14,949	16,284
Financial Institutions	1,655	7,006	14,712	12,637
Intermediaries	1,018	1,405	1,656	2,810
Total	10,067	20,698	31,317	31,731



Counterfeit Currency Reports

PML Rules 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 Counterfeit Currency Reports (CCRs) are furnished online in the revised format.

Trends in CCRs

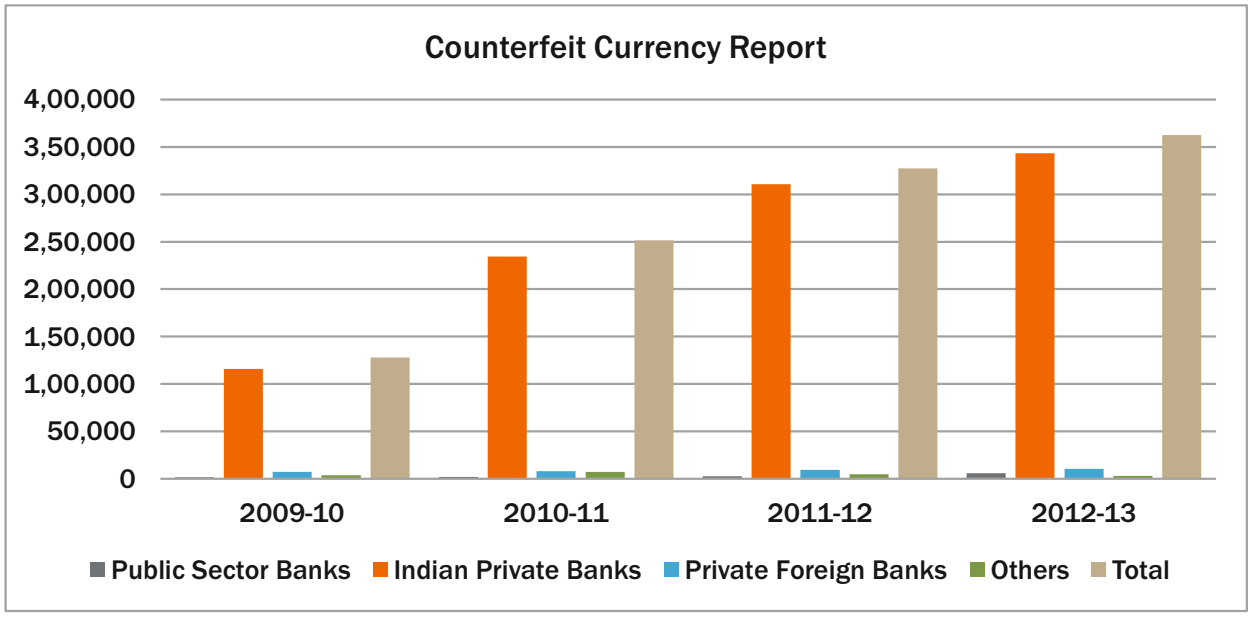
Around 11% growth in CCRs received during 2012-13 as compared to 2011-12.

Indian Private Banks continued to file more than 90% of the total number of CCRs.

As of March 2013, FIU-IND has received information about 10,67,295 incidents of detection of Fake Indian Currency Notes (FICN) with a face value of over Rs. 81 Crore.

Table 4: Receipt of Counterfeit Currency Reports from the Banking Companies

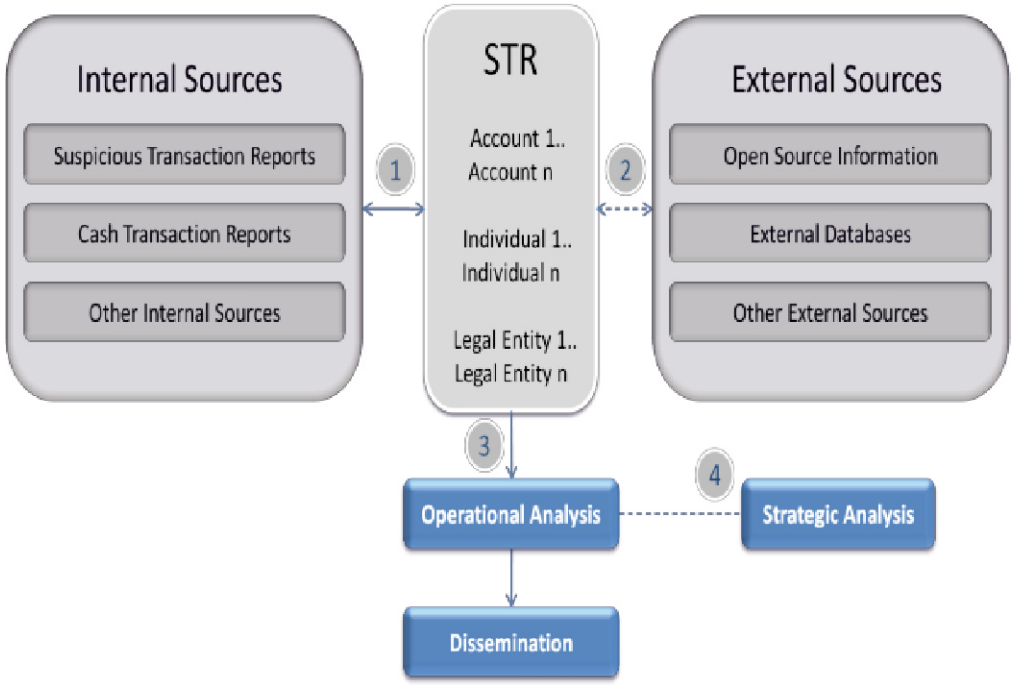
Reporting Entity Type	2009-10	2010-11	2011-12	2012-13
Public Sector Banks	1,391	1,896	2,649	5,707
Indian Private Banks	1,15,720	2,34,400	3,10,714	3,43,358
Private Foreign Banks	7,099	7,936	9,273	10,489
Others	3571	7216	4,746	2,817
Total	**1,27,781**	**2,51,448**	**3,27,382**	**3,62,371**



The private Indian Banks contributed majority of CCRs (Table 4). The compliance levels of the public sector banks continued to be low despite matter being taken up with the RBI. During the review of the public sector banks the best practices of private Indian banks in detection and reporting of counterfeit currency notes were highlighted.

Analysis of STRs

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



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

Facts reported in the STR were linked with other internal/external information and interpreted with a view to identify underlying information relevant to a partner agency. Appropriate use of technology for searching and linking the additional information (such as related addresses, individuals, entities and accounts) in respect of subjects of STRs was made through an in-house search engine. The new capabilities built in FINcore (analysis module of Project FINnet) for effective relationship resolution and linking of records has provided necessary impetus to the analysis function in the FIU-IND.

While analysing an STR, the following factors are considered for deciding whether the STR should be disseminated and if so, to which agency.

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

Table 5 : Analysis of Suspicious Transaction Reports

Category	2009-10	2010-11	2011-12	2012-13
STRs received	10,067	20,698	31,317	31,729
STRs brought forward from previous year	476	1,118	1,775	1,813
STRs Processed	9,425	20,041	31,279	18,666
STRs Disseminated	6,571	13,744	23,689	13,854

Dissemination

With the launch of the FInnet in October 2012, the STRs are processed using its FINcore system. A case is formed around an STR linking all relevant information/ reports available in the data base. Based on the grounds of suspicion and the information linked with the STR, FIU-IND decides the intelligence/ law enforcement agencies to which the case should be disseminated along with the levels of priority and feedback for each case disseminated.

Table 6: Dissemination of Suspicious Transaction Reports

Agencies	2009-10	2010-11	2011-12	2012-13
Law Enforcement Agencies	6,537	8,826	16,905	12,497
Intelligence Agencies	362	5,523	10,905	3,730
Regulators & others	128	127	225	192
Total	**7,027**	**14,476**	**28,035**	**16,419**

Note: Some STRs are disseminated to more than one agency and hence, the number of dissemination reports is higher than the number of STRs disseminated.

Dissemination of actionable and relevant financial intelligence enables FIU-IND to strengthen the work of partner law enforcement and intelligence agencies. Some of the STRs were also disseminated to financial sector regulators and foreign FIUs. Statistical information relating to dissemination of intelligence reports during the year 2012-13 is given in Table ***6***.

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

Case Study: Multi-level Marketing (Ponzi) fraud and diversion of money outside India.

Two Singapore based companies in collaboration with several Indian entities have deceived Indian public of huge amount of money through a multi-level marketing (Ponzi) scheme fraud. The companies sold subscription of an online magazine called E-magazine Survey against one-time payment of INR 11,000 (USD 180 approx.). The subscribers (called panelists or members) were given a login ID and password through which they could access the e-magazine website and participate in online market survey once a week. The company reportedly promised to pay US dollar 17 or INR 1,000 for each survey. A subscriber could participate in more than one survey every week by making multiple subscriptions of INR 11,000 up to INR 99,000. A subscriber could also mobilize other subscribers for the e-magazine and in return get 15 % bonus for each survey undertaken by the members mobilized by him.

A large number of distributor/franchisee firms received cash from subscribers and immediately transferred the funds to three or four master distributors, who in turn transferred the money out of the country through foreign outward remittances to two companies registered in Singapore and one in Italy having, directors / authorized signatories. One of the companies registered in Singapore is wholly owned by a company registered in British Virgin Islands. Master distributor companies in India and the companies in Singapore and Italy had common beneficiaries. They had common people in the management team. Their bank accounts were also held by common individuals. Indian office of the company registered in Italy had the same address as that of one of the master distributors of the scheme in India.

It is estimated that the above companies perpetrated a fraud of more than INR 23-24 billion (USD 400 million approx.) on about 2 million subscribers in India and remitted a large part of it (at least USD 120 million) to the companies in Singapore which in turn remitted part of the proceeds to the company registered in Italy.

A number of banks filed STRs in respect of the entities and individuals involved in this fraud. FIU-IND could link from its database a number of bank accounts having substantial cash transactions to the entities and individuals involved in the STRs. Valuable information about the companies incorporated outside India such as details of their incorporation, ownership, management and details of their bank accounts, transactions and fixed deposits was obtained from foreign FIUs and disseminated to LEAs dealing with serious fraud, foreign exchange violations, money laundering and tax evasion as well as to Police departments of various States of India.

The feedback from the law enforcement agencies indicates that the information supplied by FIU-IND enabled one State Police to identify and freeze the funds collected by the accused persons in various bank accounts. Another State government has registered a case for cheating under Indian Penal Code and for violation of Prize Chits Money Circulation Scheme (Banning) Act, 1978 and the case is being further investigated. Several thousand people had joined this scheme as subscribers. Those persons who got huge commission through the scheme have been made accused in the case. While in some States investigation has been completed and charge-sheets have been filed against the persons involved, the investigation is still going on in others.

The Income Tax Department has found that the Singapore based companies received through three Indian parties, remittances of more than USD 100 million as proceeds of subscription to E-magazine. At the time of enquiry, a sum of USD 22 million was found in 3 bank accounts of these parties. Action was taken under the Income Tax Act, 1961 to freeze these bank accounts. Tax assessment order for 2010-11 was passed in India against one of the Singapore based companies assessing its taxable income at USD 38 million. A tax demand of INR 19 million has been raised. Interest and penalty for failure to withhold tax has also been levied in the case of two master distributor companies which remitted the money collected from members to the account of the company in Singapore.

Analysis of CTR database

FIU-IND has developed capabilities to create multiple unified views of individuals, legal persons, bank accounts, etc fulfilling a given set of criteria or scenario. This ensures that all related information available about a subject can be viewed on a single page. Moreover, two large databases can be compared to find out common entities. Clusters of information based on common name, address, PAN or other criteria can be culled out from large databases. These know-hows enhance the quality of searching and linking process adopted by FIU-IND and add value to the primary reports received from the reporting entities. These analytical tools also enable FIU-IND to provide timely response to law enforcement and intelligence agencies on information requested by them in respect of bulk data.

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

The CTR database is used for:

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

National Risk Assessment

FIU-IND has been actively involved in the National Risk Assessment. Director, FIU-IND is the Member-Secretary of the AML Steering Committee (AML-SC) constituted by the Ministry of Finance under the Chairmanship of Additional Secretary (Revenue).

The terms of reference of the committee include:

(a) To conduct periodic assessments of money laundering risks with regard to various financial products and services, financial sectors, geographies and jurisdictions.

(b) To conduct objective assessment of the effectiveness of the implementation of the Prevention of Money Laundering Act and to identify possible legislative and administrative deficiencies

With a view to carry out the National Risk Assessment, the AML-SC has constituted three separate sector-specific Working Groups for the Banking, Insurance and Capital Market Sectors, which will assess the money laundering risk of the given sector. FIU-IND is the Convener of these Working Groups. Moreover, a sub-group has been formed under Director, FIU-IND to study various methodologies for National Risk Assessment, including the World Bank and the IMF Methodologies, for their suitability to the Indian conditions.

Ministries, departments and agencies involved in the National Risk Assessment:

- Department of Revenue (DoR)
- Department of Economic Affairs (DEA)
- Enforcement Directorate (ED)
- Financial Intelligence Unit – India (FIU-IND)
- Central Board of Direct Taxes
- Directorate General of Revenue Intelligence (DGRI)
- Directorate General of Central Excise Intelligence
- Directorate General of Foreign Trade
- Serious Frauds Investigation Office
- Reserve Bank of India (RBI)
- Securities and Exchange Board of India (SEBI)
- Insurance Regulatory and Development Authority (IRDA)

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

A. Preventing misuse of the financial system

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.

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

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

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

One of the main functions of FIU-IND is to analyse and add value to the reports received from the reporting entities. Cases considered useful are disseminated to the law enforcement and intelligence agencies for appropriate action. As many STRs are found to be false positives due to partial matching of names, enhanced due diligence is conducted by FIU-IND. In addition, FIU-IND also supports the efforts of domestic intelligence and law enforcement agencies against terror financing by providing information specifically requested by them, either by searching its database or by calling specific information from the reporting entities (Table 7).

Table 7 – Requests received from Intelligence Agencies

Category	2009-10	2010-11	2011-12	2012-13
Requests received from Indian intelligence agencies	226	428	473	457

D. Information exchange with foreign FIUs on terrorism financing cases

FIU-IND is regularly exchanging information with foreign FIUs over Egmont Secure Web on suspected money laundering and terrorist financing cases. FIU-IND has MOUs with 19 countries. MoUs with four more countries were signed in 2012-13. FIU-IND and also initiated the process to enter into MOUs with other foreign FIUs for further cooperation and exchange of information.

E. Contribution to global efforts to combat financing of terrorism

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

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

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

Chapter 4

Domestic and International Cooperation - Building Partnerships

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

During the year, FIU-IND continued to maintain close professional relationship with partner agencies based on mutual trust and understanding. An information exchange module (FINex), which was developed as part of the Project FINnet, has been made operational. The exchange module has functionality for uploading bulk requests by the domestic agencies. Greater use of this platform will ensure timely availability of information to the partner agencies and also considerably enhance FIU's ability to respond faster to the requirements of the agencies.

Several workshops were held to explain to the users of domestic agencies the framework of FINex. Demonstration of the bulk request utility with sample data to generate XML and input XML was also given to the participants.

Scope of Framework of FINex

- Authorized users
  - User Roles
- Registration process of Nodal Officer and alternate nodal office
- Features of FINnetExchange Portal (FINex)
- Spontaneous dissemination
  - Rules of spontaneous exchange
- Request based dissemination
  - Conflict resolution
  - Seeking anonymity
- Availability of Data and Statistics
  - Optimizing resource allocation
- Feedback Mechanism

Virtual Office: An effective model for exchange of information

Pursuant to the directions of the Finance Minister a Virtual Office was constituted by the Department of Revenue vide their O.M. No. M.11014/9/2012- SO (ES Cell) dated 03.01.2013. As per the Order, the Virtual Office is comprised of one representative each from CBDT, DGCEI, DGRI, CEIB and FIU-IND. The terms of reference of the Virtual Office include:

(i) Creation of a Closed User Group (CUG) on NIC email portal for exchange of information among the members of the Virtual Office.

(ii) Member agencies to capture feedback on STRs from their field units using the prescribed feedback format of FIU-IND.

(iii) Aggregated information in an Excel sheet to be periodically submitted to FIU.

(iv) Monthly reporting of the feedback received to Revenue Secretary / Finance Minister.

A Closed User Group (CUG) on the NIC mail portal has since been created and actively used by the members. The Virtual Office has also designed a spread-sheet for capturing macro level information about the usefulness of an STR. The template is being used by the members for reporting feedback to FIU-IND. The Virtual Office has proved to be an effective model for exchange of information mainly among the tax agencies.

Law enforcement/ intelligence agencies

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

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

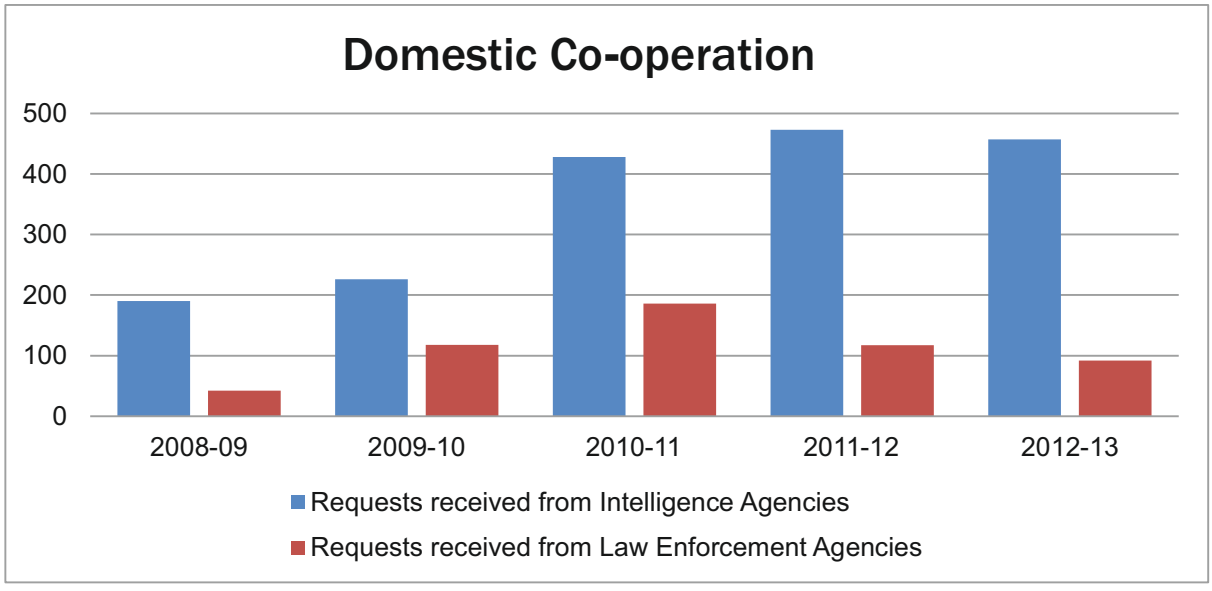
FIU-IND actively participated in meetings of Central Economic Intelligence Bureau (CEIB) and Regional Economic Intelligence Councils (REICs) to discuss issues of common interest. FIU-IND also interacts with the

nodal officers of law enforcement agencies of the state governments and union territories on regular basis.

FIU-IND's database on cash and suspicious transactions are found very useful by domestic law enforcement and intelligence agencies. The partner agencies relies on information contained in FIU-IND databases not only for developing intelligence but also for strengthening ongoing investigations. During the year, FIU-IND provided timely information to various agencies in response to 549 references on money laundering, terrorist financing, corporate frauds, organized crimes, fake Indian currency, tax evasion etc. ***(Table 8)***.

Table 8 : Number of references from domestic law enforcement/ intelligence agencies

Category	2008-09	2009-10	2010-11	2011-12	2012-13
Requests received from Intelligence Agencies	190	226	428	473	457
Requests received from Law Enforcement Agencies	42	118	186	117	92



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

Memorandum of Understanding (MOUs)

Memorandum of Understanding (MOU) is a statement of intent for extending cooperation and mutual exchange of information entered between the two organizations and is not a legally binding document. 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. The MOU is also necessitated due to the fact that the information disseminated by FIU-IND is extremely sensitive and, therefore, it is important that it is protected from unauthorized use and proliferation and the provisions of confidentiality and data protection are applied throughout the chain of transmission of information of FIU-IND to the agencies receiving the information. During the year, it was proposed to review the existing MOUs signed with the domestic agencies and enter into new MOUs with other agencies. The new proposed MOU aims to provide a framework for standard operating procedure (SOP) for handling information received from FIU-IND by the authorized agencies. It is also planned to have similar MoUs with the regulators of financial sector (RBI, SEBI, IRDA and PFRDA).

Regulators

FIU-IND has also developed close relationship with financial sector regulators for strengthening AML and CFT regulations. The regulators, namely, Reserve Bank of India (RBI), National Bank for Agricultural and Rural Development (NABARD), Securities and Exchange Board of India (SEBI) Insurance Regulatory Development Authority (IRDA), National Housing Bank (NHB) and Pension Fund Regulatory & Development Authority (PFRDA) have issued instructions to the financial sector entities for adherence to KYC, AML and CFT norms. FIU-IND has ensured that suitable modifications are carried out in the circulars, wherever necessary. These circulars are also uploaded on the website of FIU-IND for quick reference.

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

Global AML/CFT efforts

FIU-IND continued with its strategy to foster strong relationship with the FIUs of other countries, including the neighbouring countries. During 2012-13, the level of exchange of information with foreign FIUs continued to be high. With a view to formalizing the nature and scope of mutual co-operation, FIU-IND initiated the process of signing of MoUs with several countries. FIU-IND also continued to actively participate and contribute in the activities of various regional and international bodies dealing with AML/CFT issues.

FIU-IND is providing technical assistance to FIU Bhutan for establishing an electronic reporting system. The necessary hardware for technical solution has been made available to FIU Bhutan and a team of FIU-IND officials will shortly visit Bhutan to install the application software and to provide basic training to the users.

FIU-IND representatives have been regularly participating in the meetings of the Financial Action Task Force (FATF) and its working groups. During 2012-13, an Additional Director in FIU-IND participated in the Rome plenary of the FATF in June, 2012. Another Additional Director represented India in the proceedings of the Working Group on Evaluation and Implementation (WGEI) of the FATF at Paris in February, 2013 and participated in the discussion and finalization of the Methodology for Assessment of Technical Compliance and Effectiveness.

FIU-IND has been participating in the meetings of Contact Group on Piracy off the coast of Somalia (CGPCS), which is a body created by the United Nations Security Council for combating maritime piracy in the Gulf of Aden and other areas off the coast of Somalia. During the year 2012-13, India held the Chair of CGPCS and FIU-IND actively participated in the meeting of the heads of the five Working Groups of CGPCS held at New Delhi and in the preparation of the plenary of CGPCS at New York in December, 2012. FIU-IND also shared critical information relating to suspected ransom payments to Somali pirates using the Indian financial system.

FIU-IND officers have also been representing India in the meetings of the Sub-Group on Combating Financing of Terrorism of the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC), which is an international organisation involving a group of countries in South Asia and South East Asia.

Financial Action Task Force

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

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

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

FIU-IND has actively participated in the activities of the Financial Action Task Force (FATF). Officers from FIU-IND were a part of the Indian delegation to FATF and attended the FATF meetings in June 2012 at Rome, Italy and in October 2012 and February 2013 at Paris, France.

A senior officer of FIU-IND attended the meetings of the 'Sub-Group of FATF on Effectiveness' and meetings of the FATF members on 'Risk & Threat Assessment' in April 2012 at Singapore. These meetings were critical in the evolution of the Assessment Methodology for AML/ CFT Effectiveness and the FATF Guidance Document on National Money Laundering and Terrorist Financing Risk Assessment later in the year.

In February 2013, FATF issued the Guidance document on National AML/ CFT Risk Assessment so as to facilitate and guide countries to carry out National Risk Assessment (NRA), which will act as the basis for the Risk Based Approach (RBA). With a view to implement RBA and carry out the NRA, the AML Steering Committee (AML-SC) was constituted by the Central Government in the Department of Revenue, Ministry of Finance in February, 2012 with Director, FIU-IND as its Member-Secretary. On the suggestions of the AML-SC, FIU-IND conducted a workshop on Risk Based Approach in September, 2012, which was attended by about 50 representatives from banks and other financial institutions as well as intelligence and law enforcement agencies.

FATF Style Regional Bodies (FSRBs)

There are 8 FSRBs which provide leadership in their regions and are an important means of promoting

consistency in application of the FATF standards. India is a member of 2 FSRBs, the 40-member Asia Pacific Group (APG) and the Eurasian Group (EAG). India's joining of EAG in December, 2010 has been instrumental in further strengthening of regional cooperation in combating money laundering and the financing of terrorism. FIU-IND has been an active participant in the activities of APG and EAG.

FIU-IND delegates fully engaged themselves in the deliberations of the EAG plenary held at New Delhi in December, 2012 and the issues of mutual co-operation between the FIUs of the EAG member countries emerging from the deliberations, especially in the area of crimes relating to drug trafficking, are consistently followed up by FIU-IND.

An Additional Director made a presentation and led the discussions on maturity assessment of FIUs and strategic analysis at the FIU Forum of ESAAMLG, a FATF styled regional body, at Arusha, Tanzania.

The 16th Annual Meeting of APG and the meeting of the Technical Assistance Forum were held at Brisbane, Australia, which was attended by Director, FIU-IND.

A senior officer of FIU-IND participated in the meeting of FATF/ GIABA Joint Experts Workshop on Money Laundering and Terrorist Financing Typologies held at Dakar, Senegal in November, 2012.

FATF Mutual Evaluation of India and the Follow-up Process

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

Follow-up Process and Recommended Action for FIU-IND

Table 9: Action suggested in Mutual Evaluation Report 2010 of India

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

Though India was admitted as a Member of the FATF in June 2010, it was put under a follow-up process with regard to the deficiencies pointed out in the MER. Accordingly, India drew up an Action Plan for addressing the deficiencies in the short term (before 31.03.2011) and the medium term(before 31.03.2012). With regard to the FIU-IND, the actions required to be taken are listed in ***Table No.9.***

FIU-IND took systematic and concrete steps in the areas of deficiency to become compliant with the FATF standards. The action taken on the specific suggestions of FATF are listed in ***Table No. 10.***

A technical team of the FATF visited India during 11-18 April 2011 to review the efforts made by FIU-IND for removing the deficiencies pointed out in the MER. The review team's overall impression was that India is strongly committed to the FATF process and to the implementation of an effective AML/CFT framework. With regard to the progress made by FIU-IND, the team observed that FIU-IND is to be commended on the efforts that it has made over the past year to pick up on the points made in the MER, to monitor the trends in STR filing, and to be proactive in its direct engagement with the reporting institution. The effect appears to have been a markedly improved reporting regime.

FIU-IND continued to make further progress in the areas of enhanced outreach, extensive compliance monitoring, reporting of terrorist financing related STRs, identification and prescription of more red flag indicators, streamlining of the feedback mechanism, etc., which has been acknowledged by the FATF in various Follow-up Reports.

The FATF on-site team also acknowledged that the FIU is well advanced in the development of its FINnet system, which will provide for real-time filing of STRs by all reporting institutions. The FINnet system has since been implemented by FIU-IND and has significantly enhanced the efficiency and quality of reporting and the analytical capabilities of the FIU.

FIU-IND has also undertaken extensive outreach to the financial institutions by way of seminars and training workshops, which have included special programmes on terrorist financing. In the past year, FIU personnel have provided their expertise in 38 training programmes involving over 2,800 participants, and have also run a Train-the-Trainer course for 63 key resource persons from various training colleges of banks and other financial institutions. The FIU continues to undertake focused reviews the level of compliance of the reporting entities with the statutory reporting obligations in both the public and private sectors. These efforts have resulted in a significantly improved reporting regime.

Egmont Group of FIUs

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

The membership of Egmont Group has increased to 131 as on 31st March 2013. Member FIU undertake to subscribe to the Egmont Group principles. The member FIUs work for co-operation and exchange of information 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.

Table 10: Summary of Action Taken by FIU-IND

Recommendation	Action taken by FIU-IND
R 12, R 16, R 24 (Designated Non-Financial Businesses & Professions)	1. A Casino Sector Assessment Committee (CSAC) was constituted under the chairmanship of Director (FIU-IND) which carried out a comprehensive review of the Casino Sector. The Committee has made several recommendations to the Government for strengthening the AML/CFT regulatory framework for this sector including- • Creation of comprehensive legal framework. • Autonomous regulators or Gaming Commissions for casinos. • Cooperation between regulators of different States. • Effective 'fit and proper' test. • Review of current KYC threshold to align it to FATF standards. • Issue of comprehensive AML/CFT guidelines. 2. Several outreach programmes were conducted by FIU-IND for ICAI and ICSI during August 2010- March 2011, which were attended by 230 Chartered Accountants and 558 Company Secretaries. 3. FIU-IND approached ICAI, ICSI and ICWA for inclusion of modules on AML/CFT in the curriculum of their courses and offered assistance and guidance in updating the course contents. 4. A training workshop on Combating Financial Crime was organized by the Institute of Company Secretaries of India (ICSI) in March 2012, which was addressed by a senior officer of FIU-IND. 5. FIU-IND officers conducted another outreach programme with the Institute of Chartered Accountants in June, 2012, which was attended by 54 participants. The participants were given exposure to the international AML/ CFT standards and the AML/CFT regime in India along with inputs on methods to address AML/ CFT risks by the financial institutions.
R13, SR IV (Suspicious transaction reporting)	• FIU-IND has, in consultation with RBI and IBA, identified red flag indicators to detect suspected TF cases. • An analysis of the adequacy of STRs related to different sectors and geographies was carried out by FIU-IND. • A special review of AML compliance level by the private sector banks has been done by FIU-IND and 11 banks have been identified for close monitoring of their reporting system. • Advisories have been issued to 323 Reporting Entities during 2010-11 for improvement in number and quality of reporting. • Penalties have been imposed on two banks for failure to put in place a satisfactory system for identification and reporting of suspicious transactions. • FIU-IND has been encouraging the reporting entities to conduct in-house training on AML/CFT for their own employees. Feedback received from 31 training colleges of banks, which attended the "Train the Trainer Workshop" held on 29.9.2010, shows that these colleges have conducted 1,981 training programmes on AML/CFT, attended by 59,267 bank employees. 1,896 of such training programmes included a specific module on Terrorist Financing. • FIU-IND is in dialogue with Indian Institute of Banking & Finance (IIBF) for expanding outreach in the banking sector. IIBF has been conducting a certificate course in "Anti Money Laundering and KYC Guidelines" since 2005 and 13,031 candidates have been given certificates. • The number of TF related STRs has increased in 2010-11 to 259, which is a 100% increase over 2009-10 figures. • An analysis of the adequacy of STRs related to different sectors and geographies has been completed by FIU-IND based on the data of STRs received up to March 2010. The final report has been published by FIU-IND. • A special review of AML compliance level by the private sector banks has been done by FIU-IND and 11 banks have been identified for close monitoring of their reporting system. • Advisories have been issued to 323 Reporting Entities during 2010-11 (as against 237 in 2009-10 and 214 in 2008-09) for improvement in number and quality of reporting. • Penalties have been imposed on two banks for failure to put in place a satisfactory system of identification and reporting of suspicious transactions. • A Working Group consisting of select banks along with RBI, IBA and FIU-IND was formed to help banks to evolve common platform/practices in dealing with KYC/AML related issues under PMLA, 2002 and suggest standard parameters for all banks to generate suspicious transactions. The Working Group submitted its report in March 2011 which has been circulated to banks vide IBA's circular dated May 18, 2011 for information and implementation. • Several rounds of meetings have been held with the intelligence agencies to assess the effectiveness of STRs related to Terrorist financing and identify red flag indicators to detect suspected TF cases.
R 26 (Financial Intelligence Unit)	• A report on trends of STRs has been compiled and published. • FIU-IND has held regular meetings with nodal officers of central law enforcement agencies and state police. • FIU-IND conducted several training sessions covering 'AML/CFT regime and role of FIU-IND' for officers of central and state law enforcement agencies. • FIU-IND organized an interactive session with representatives of the law enforcement and intelligence agencies to present the implementation roadmap of Project FINnet • FIU-IND participated in five training programmes organized by the CBI Academy and the National Academy of Customs Excise and Narcotics (NACEN) on a range of AML related topics which was attended by around 138 officers of central and state law enforcement agencies. • FIU held meetings in five state capitals to interact with the senior officers of state police. The interactions have further strengthened the mechanism for information sharing. • FIU-IND held 3 meetings with the intelligence agency and the law enforcement agency, to whom the largest number of STRs are disseminated, to apprise them of the progress in the implementation of Project FINnet and to explain the role and responsibilities of the agencies under the new system. • During 2011-12, 34 trainings were organized for the law enforcement authorities on various issues of AML/ CFT, which were attended by 1,422 officers of these agencies.

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 20th Annual Plenary session of Egmont Group at St. Petersburg, Russia in July 2012 and the Egmont Working Group at Ostende, Belgium in January 2013. FIU-IND has been spear-heading a project on FIU Information System Maturity Model (FISMM) which was initiated in 2009. The FISMM project was approved by the Heads of FIUs for implementation during the St. Petersburg meeting of the Egmont Group.

FIU-IND Officials have been actively participating in Operational Working Group (OpWG), Training Working Group (TWG) and IT Working Group (ITWG) of the Egmont Group. Leadership in FISMM project gives FIU-IND an important role in defining the emerging standards for assessment of effectiveness of FIUs.

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

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

Director, FIU-IND is a member of the Legal stream and has been regularly contributing in the finalization of various issues identified by CRP for detailed examination. This has given FIU-IND the unique opportunity of participating, for the first time, in the standard setting process of the Egmont Group. In this process, FIU-IND has contributed detailed papers on all the issues assigned to FIU-IND and also provided substantive comments on the other issues dealt with by the other countries.

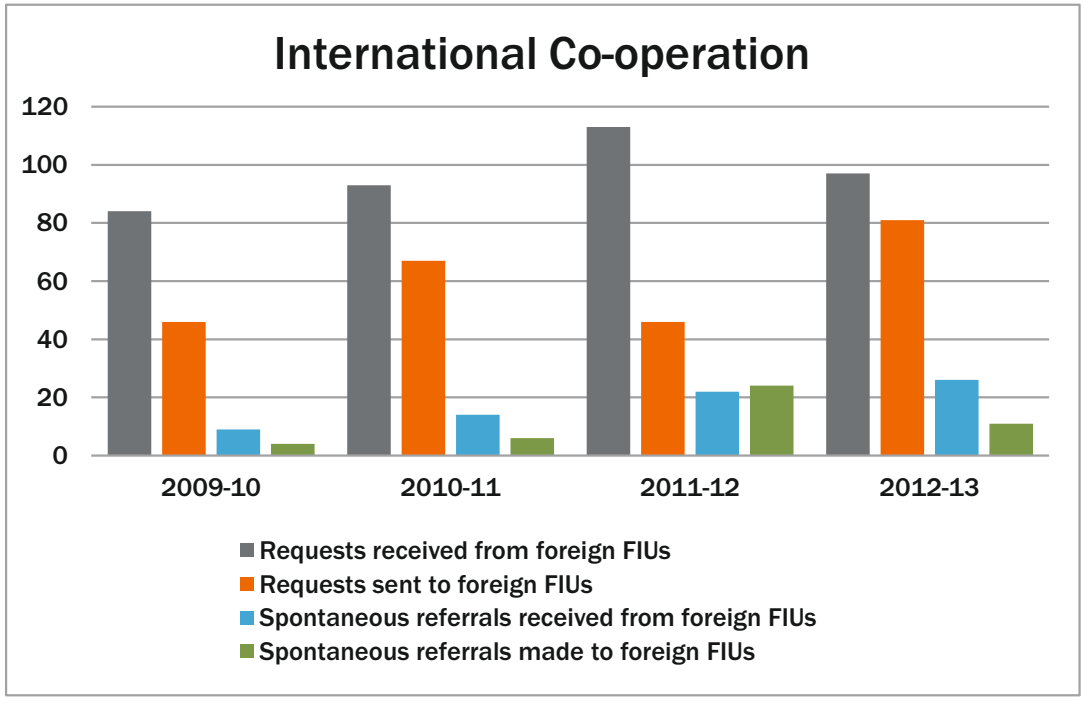
Co-operation and exchange of information with other FIUs

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

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

Table 11: Exchange of information with foreign FIUs

Status of action Taken	2009-10	2010-11	2011-12	2012-13
Requests received from foreign FIUs	84	93	113	97
Requests sent to foreign FIUs	46	67	46	81
Spontaneous referrals received from foreign FIUs	9	14	22	26
Spontaneous referrals made to foreign FIUs	4	6	24	11



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 negotiating MoUs with various FIUs during the year. MoUs with more than 15 countries are under various stages of negotiation.

Joint Working Groups on Counter Terrorism

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

Chapter 5

Raising awareness and building capacities of reporting entities

The number of entities operating in the financial sector in India is very large and it is a challenge to engage them and ensure their compliance with the reporting obligations. The success of an FIU depends largely on the ability of reporting entities in effectively identifying and reporting transactions. FIU-IND continued its focus on increasing awareness of the reporting entities about their reporting obligations under PMLA and building their capacities to ensure better compliance.

A significant step taken in enabling the reporting entities to efficiently identify suspicious transactions and report them to FIU was to prescribe a standard set of Red Flag Indicators (RFIs) for the banking sector in July, 2011 in collaboration with RBI and IBA. On the same lines Working Groups were formed for payment system operators and money transfer service providers and on the basis of their reports, RFIs have been circulated for payment system operators and money transfer providers in October, 2012. The Red Flag Indicators:

- Create a common and shared understanding aligned with global norms and practice about the implementation of STR detection and reporting systems.
- Provide indicative lists of high risk customers, products, services and geographies.
- Provide a list of commonly used alert indicators for detection of suspicious transactions.
- Provide guidance for an effective alert management and preparation of STRs.

As in earlier years, FIU-IND adopted a multi-pronged strategy to enhance awareness through the FIU's

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

FIU website

The FIU-IND websites (http://fiuindia.gov.in and http://finnet.gov.in) are user-friendly sites 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 e-filing of reports on the FINnet portal for use by the smaller reporting entities that have limited IT infrastructure. These utilities are available for free download on the FIU-IND website http://finnet.gov.in.

Seminars and workshops

During the year, FIU-IND participated in 38 workshops/interactions on AML/CFT awareness in collaboration with regulators, industry associations, professional bodies and reporting entities, targeted at over 2,800 participants. The statistics relating to training seminars and workshops are in ***Table 11.***

During the year, FIU-IND focused on training the reporting entities in various sectors on online filing of reports on the FINnet portal. Besides this, FIU-IND also focused this year on enhancing awareness of cooperative banks about their reporting obligations under the PMLA among authorized dealers/Full Fledged Money Changers (FFMCs) and Money Transfer Service Scheme (MTSS) operators and their agents who were inducted as reporting entities recently.

Twenty eight review meetings were conducted for the CEOs/Chairman/Principal Officers of the reporting entities in various sectors covering 1471 officers.

Table 11: Outreach Activities

Outreach Activity	2009-10	2010-11	2011-12	2012-13
Seminars and Training workshops	76	50	42	38
Number of Participants	3,145	2,264	2,509	2862

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

'Train the Trainers'

Financial Intelligence Unit-India(FIU-IND) organized a one day "Train the Trainers" workshop on AML/CFT at India Habitat Centre, Lodhi Road, New Delhi on 5th October, 2012. This was sixth consecutive annual workshop organized by FIU-IND for the trainers. 63 senior officers of the public and private sector banks, insurance companies, government departments such as India Post, National Savings Institute and faculty members of staff training colleges and institutes of banks and professional bodies such as ICAI, ICWAI etc. attended the workshop. They are expected to act as resource persons for training other officers and staff of their respective organizations on the AML/CFT/KYC issues. The focus of the workshop was to make the resource persons aware of the latest developments in the field of AML/CFT regime such as proposed amendments to PMLA, revised FATF guidelines, risk based approach for effective detection of suspicious transactions and discuss KYC standards. To present a regulatory perspective on KYC standards, Shri S. K. Jha, Deputy General Manager, RBI addressed the session. Shri Vikas Tandon, Director-AML, Citi Bank, addressed the session on the AML/CFT Training Needs Assessment and Effective Training Delivery. With a view to give both practical and theoretical inputs, a session on STR typologies was also included this year. Each presentation was followed by an interactive session with participants. Overall feedback of the participants for the workshop was 4.25 on a scale of 1 to 5.

Chapter 6

Ensuring Compliance with reporting obligations under PMLA

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

Review meetings

FIU-IND has been undertaking periodic sector-wise reviews to evaluate the AML performance in specific sectors ***(Table 12)***. These review meetings are held with principal officers of reporting entities. The representatives of regulators and industry associations such as Indian Banks Association, Life Insurance Council and AMFI were invited to participate so that industry-specific issues could be discussed in detail, and a common understanding of issues could develop across a sector. Sector-specific meetings helped FIU-IND to evaluate the AML performance of individual reporting entities as compared with their peers, and to enable individual reporting entities to benchmark their performance. Common queries/issues of various sectors are also addressed.

Table 12 -Review Meetings with Principal Officers

Month	Meetings held with
April 2012	§ Public Sector Banks
May 2012	§ Insurance § Private Banks
June 2012	§ Public Sector Banks
July 2012	§ Private Sector Banks
August 2012	§ Urban Co-operative Banks
October 2012	§ Public Sector Banks
November 2012	§ Insurance § Private Foreign Banks
December 2012	§ Authorised Money Changers § Intermediaries § IBA
March 2013	§ Public Sector Banks § Private Sector Banks § Insurance

During the sector review meetings, the number and quality of reports submitted by individual reporting entities were analyzed to assess gaps and identify focus areas for individual entities that were not performing against the benchmarks set by their peers. Examples of sanitized cases and feedback received by FIU-IND from law enforcement and intelligence agencies were also shared during these meetings.

FIU-IND's Strategy for ensuring compliance to PMLA

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

Other compliance measures

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

FIU-INDIA has signed MOU with RBI and is in the process of signing MOUs with other Regulators. This has enabled a regular and structured exchange of information between RBI and FIU-INDIA, resulting in better compliance monitoring.

During the year, 208 advisories were issued to reporting entities highlighting problem areas and advising them to improve their compliance under PMLA. In one case, fine was imposed by FIU-IND on a reporting entity which has filed appeal before PML Tribunal.

The details of advisories issued are as under:

Table 13- Sector-Wise Statistical Analysis of Advisories issued

Sl. No	Category	2009-10	2010-11	2011-12	2012-13
1	Public Sector Bank	24	23	8	2
2	Indian Private Sector Bank	15	29	7	8
3	Foreign Private Sector Bank	3	33	0	0
4	Regional Rural Bank	12	22	800	0
5	Urban Co-operative Bank	150	206	82	0
6	Capital Market Intermediary	31	3	20	52
7	Insurance Companies	0	1	14	142
8	Other Financial Institutions	2	6	7	0
9	Finnet related issues	0	0	0	4
	Total	**237**	**323**	**938**	**208**

Table 14–Subject-wise Analysis of Advisories issued

Sl. No	Subject	2009-10	2010-11	2011-12	2012- 13
1	CCR	79	59	0	0
2	CTR	126	249	0	*
3	STR	20	13	56	*
4	KYC/AML	0	0	0	5
5	Multiple Issues (CTR,STR,KYC/AML,FINNET)*	12	2	882	203
	Total	**237**	**323**	**938**	**208**

Chapter 7

Organizational Capacity Building

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

The analysts of FIU-IND were given intensive training in IDEA® -Data Analysis Software. The data analytics allows the user to look at data from different angles has proved to be an immensely useful tool for examining compliance activities of reporting entities. Additionally, data analytics are used for reconciliations, operational analysis, and to identify unusual activity within massive amounts of data such as cash transaction reports, etc. With IDEA® - Data Analysis Software one can quickly import data from almost any source, perform 360° analytics to dig into the root cause of fraud and abuse, communicate the results and automate repeatable tasks. IDEA offers unique capabilities such as unlimited file size, impressive speed, and the ability to access and analyze large volumes of data in seconds.

The other major initiative taken during the year to enhance the capacity of the analysts was to organize talks by subject matter experts or domain experts from financial sector and allied areas. These talks are found to expand the knowledge base of analysts and provide insight into complex areas such as regulation, technology, intelligence, etc.

Training is one of the tools to equip people with necessary skills. FIU-IND has made proactive efforts to regularly upgrade the skills of its employees by providing them opportunities for training on AML/CFT and related economic issues. During the year, FIU-IND officials attended training in different areas (Table 15) including emerging payment system, revised FATF Standards, data integration, FICN, corporate frauds, financial sector supervision and AML policy development.

Table 15 : Capacity Building Workshops attended by Officers from FIU-IND

Month	Workshop	Organized by	Venue
June, 2012	Implementation of revised AML/CFT laws and procedures and combating financial crimes and terrorist financing.	U S Embassy, Bangladesh and Bangladesh (National) Bank	Dhaka
June, 2012	Emerging Payment System- Technical Capacity Building Workshop	U.S. Agency for International Development	Bangkok
June & July, 2012	Revised FATF Standards	RBI and IMF	Pune
July, 2012	Banking Laws & Fiscal Law Enforcement	State Bank Staff College	Hyderabad
July, 2012	Data Integration	IBM	Bangaluru
Sept., 2012	Prevention of smuggling of FICN & Foreign Currency	NACEN	Mumbai
Oct., 2012	Investigating Economic Crimes in Financial Markets	IICM and CEIB	Mumbai
Oct., 2012	Intelligence gathering & intelligence tradecraft	Cabinet Secretariat	Gurgaon
Nov., 2012	Expert Group on ML/TF Typologies Project	FATF	Dakar, Senegal
Dec., 2012	Enhancing international cooperation in investigation, prosecution and related matters in corruption offences	CBI	Ghaziabad
Dec., 2012	Fraud in Multi-level Marketing (MLM) entities and in Collective Investment Scheme (CIS)	CBI	Ghaziabad
Jan., 2013	AML/CFT Workshop	NACEN	Mumbai
Jan., 2013	Egmont Supervisory Course 'Pilot'	Egmont	Ottawa, Canada
Feb., 2013	Fraud in MLM, NTTS and CIS	CBI	Ghaziabad

Chapter 8

Strengthening IT infrastructure

Introduction

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

Objectives of the Project FINnet:

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

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

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

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

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

Design and Implementation Phases

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

The implementation phase started with the signing of contract with Wipro Ltd as the System Integrator on 25th February 2010. FINnet Gateway report upload module went live on 20th October 2012 and reporting entities began upload of reports in the XML reporting

format on the Gateway. The complete solution was accepted on 22nd March 2013. The SI would provide enhanced support for 1 year from the date of the acceptance of the complete solution. The enhanced support would include Administration of Databases, Systems and Network, Facility Management Services, External Users Help Desk Services and Website maintenance. The SI is also required to provide Maintenance Support for the software and hardware for an additional 2 years.

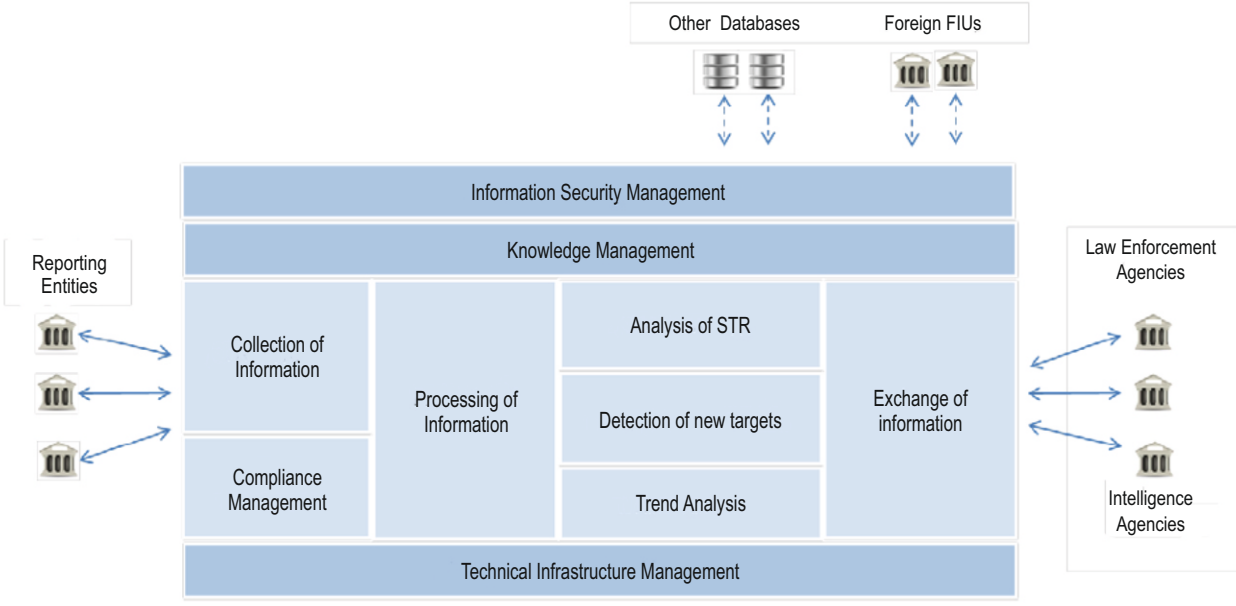


Figure: Schematic overview of FINnet

Collection of Information

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

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

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

The FINnet Gateway Portal is designed as a comprehensive interface between the reporting entities and FIU-IND to submit reports and exchange information.

The portal enables users to upload reports and download data quality reports and additional request for information. The portal also offers a comprehensive shared repository of resources like discussion forums, FAQs, problems and solutions and downloads.

Messaging module and user groups enable collaboration of users within the portal.

After the FINnet gateway module went live on 20th October 2012,the Reporting Entities started filing reports online through the portal. As of March 2013, 35 Lakh reports were filed by 1500 Reporting Entities.

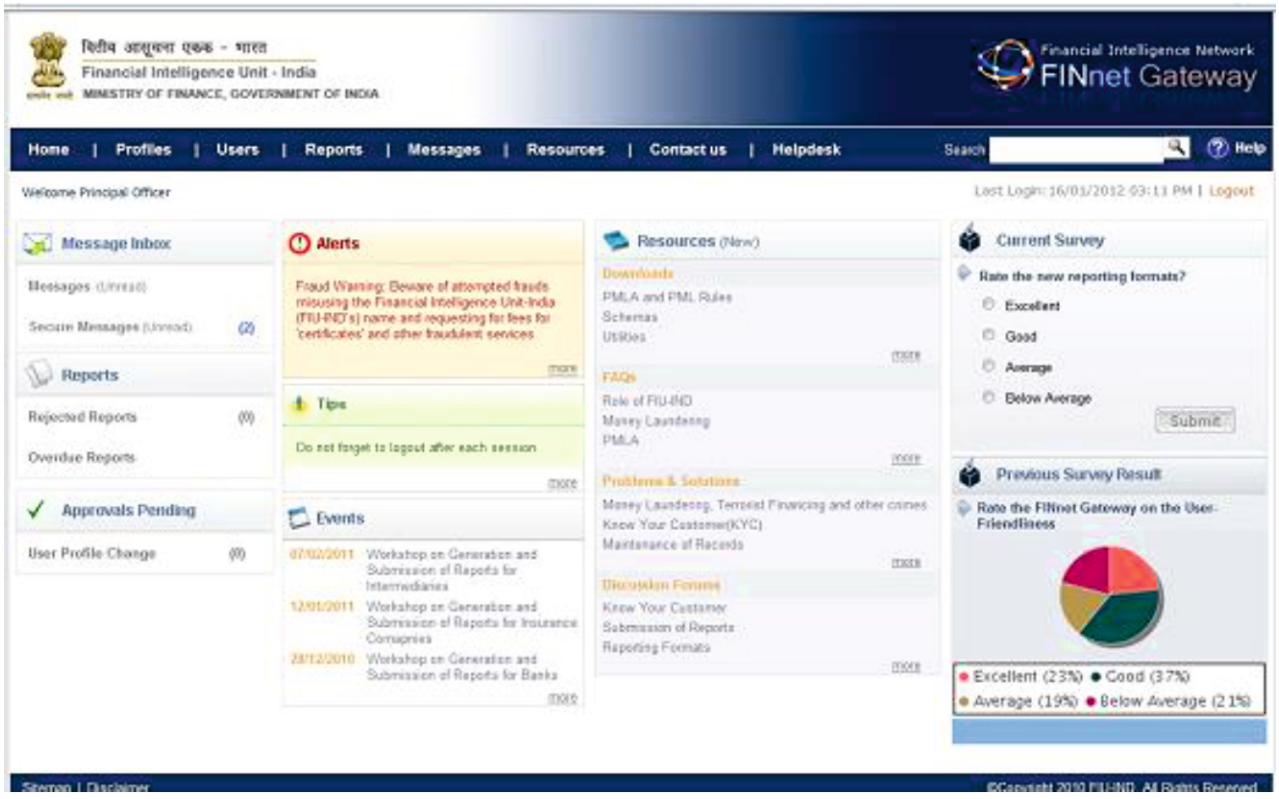


Figure: FINnet Gateway Portal for reporting entities

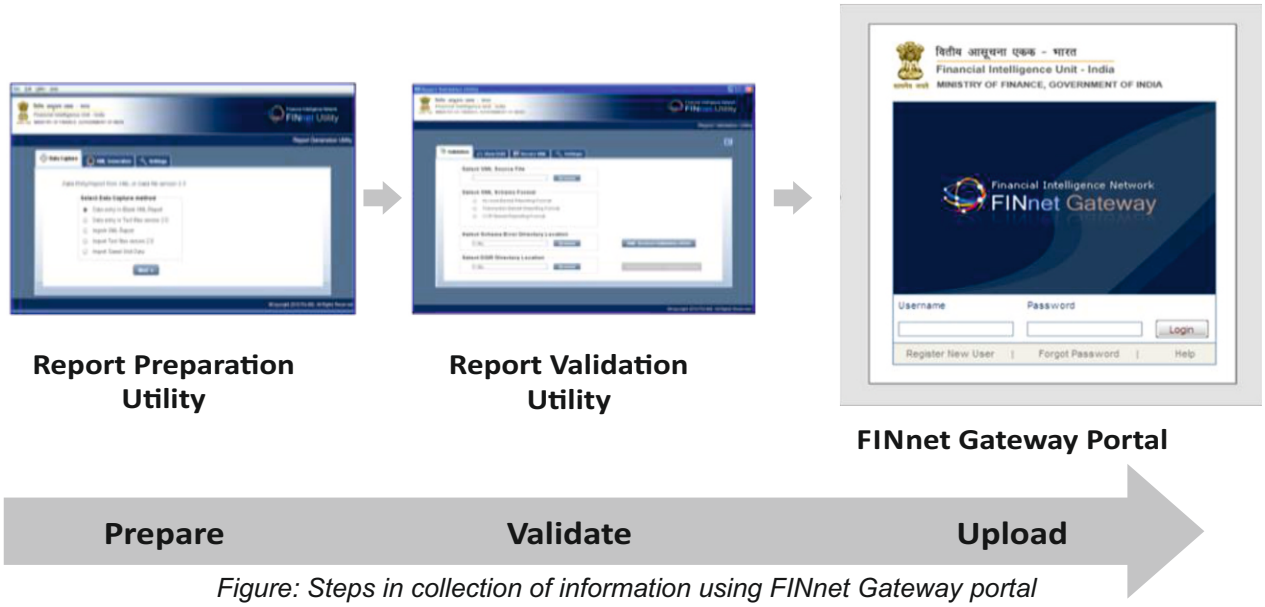


Figure: Steps in collection of information using FINnet Gateway portal

Processing of Information

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

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

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

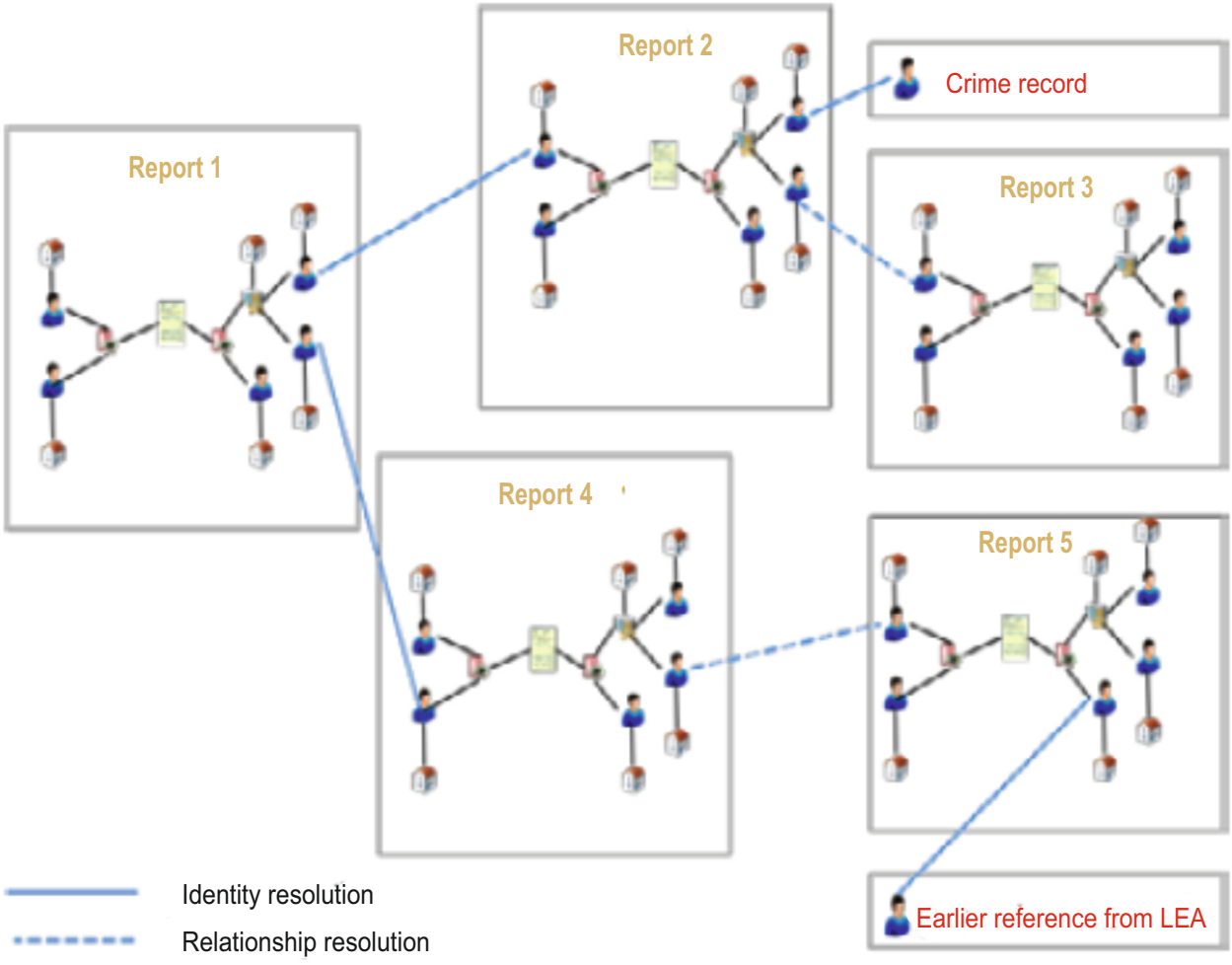


Figure: Clustering of report by Identity and Relationship Resolution.

Analysis of Reports

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

A case decision making process is enabled, wherein analyst can decide to retain or disseminate a case. In case of dissemination, the analyst can select the agencies and users for dissemination. The system also enables a staggered dissemination. The cases are published in PDF and XML format. Till march 2012 10 thousands cases were formed.

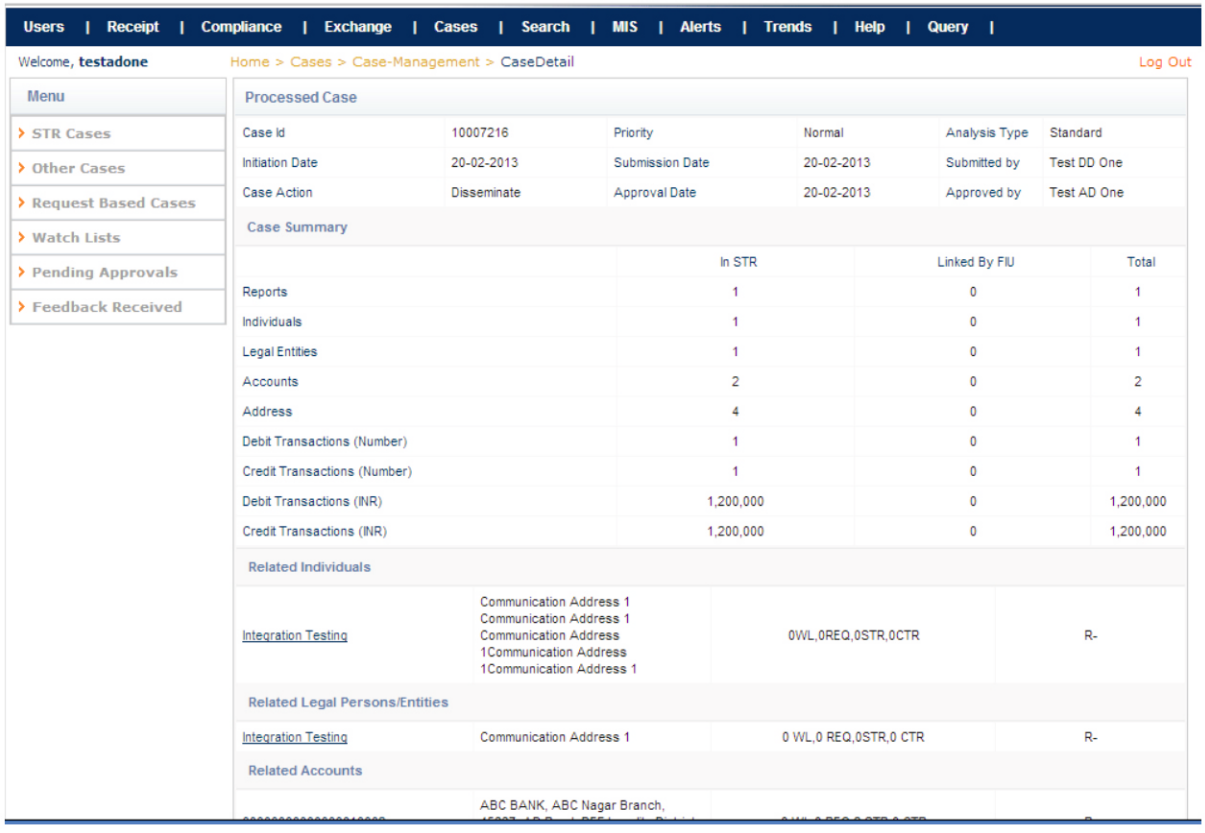


Figure: Review of STR case by Analyst at FIU

Operational Analysis of Reports (CTR,STR, NTR)

Operational Analysis of Cash Transaction Reports (CTR) are based on Alert management system which utilises the risk based approach. A comprehensive risk management system consisting of data mining tool and rules based engine is used to assess the risk in CTRs, STRs, persons, accounts, and cases using pre-defined scenarios. The risk scores are computed and aggregated using a risk based approach.

Analysis is done at two levels . One is the generation of alerts on various CTRs filed online with FIU-IND and second is identification of new target by generating list view.

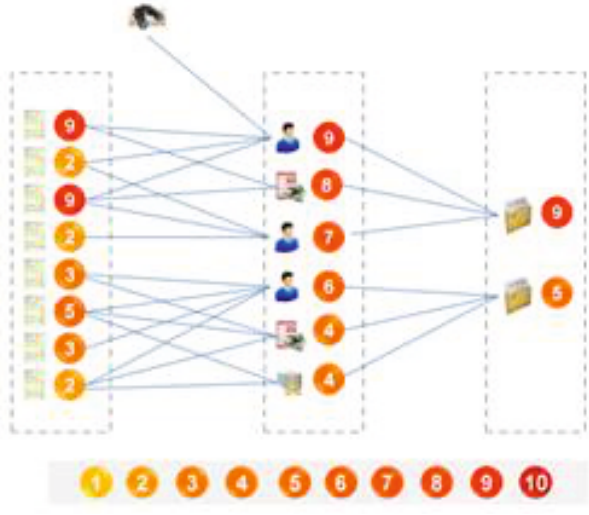


Figure: Detection of new targets at FIU

A. Generation of Alerts (Processing of CTRs):

CTRs received would be screened through the watch lists and hot lists maintained by FIU-IND.

In case the individual / legal entity reported in the CTR is part of the watch list / hot list, the CTR would be generated as an alert. The alert would also be linked with other reports in the FIU-IND database before being prioritized and assigned to an analyst.

In case the individual / legal entity is not part of the watch list / hot list maintained, the CTRs would be run through the risk based model (Det-Risk) to generate alerts (high risk CTRs) on the basis of predefined rules.

The alerts generated would be prioritized by the system cumulatively with other reports which would be verified. The prioritized alerts would be allocated by the system to the Report Preparer.

B. Identification of New Targets:

The list management module helps the analyst in detecting new targets by applying complex scenarios.The alert management system enables analysts to identify and filter high risk reports, persons, accounts, and cases using configurable thresholds. The system also enables geographical filtering at country, state, district and pin code levels. He can then generate new cases from the detected target.

Strategic Analysis

Strategic Analysis of database is build around Trend Module of Fit is based on a business intelligence software to identify trends in reports, suspicion types, counterfeit currency incidents, remittances and card transactions. The trends can be analysed over time period or geographies.

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

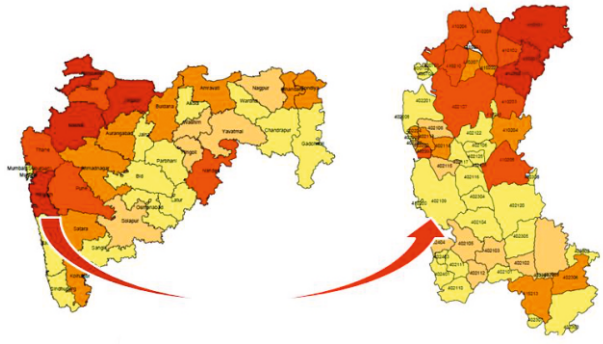


Figure: Geographical distribution with drill down

Compliance Management

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

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

Fig: Compliance related information of reporting entity

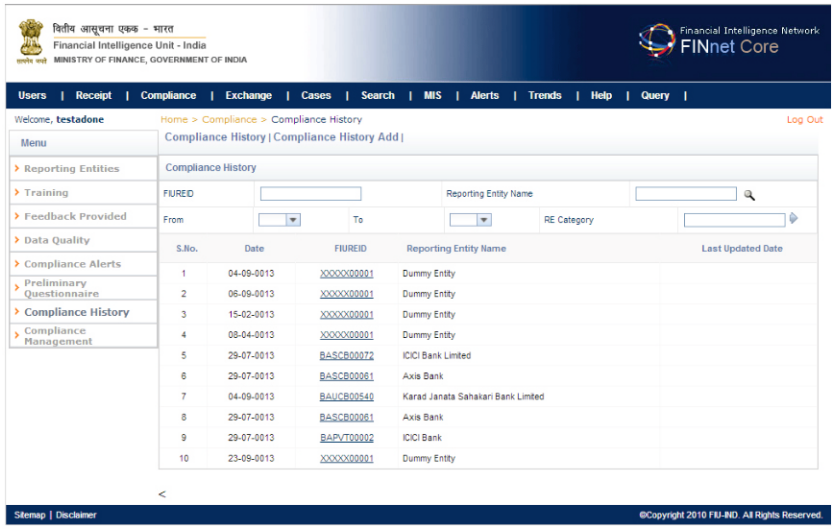


Figure: Compliance Screen in FINCORE

Exchange of information

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

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

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

Knowledge Management

FINnet includes a comprehensive knowledge managements system (KMS) to support the following

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

The KMS provides following functionalities for effective knowledge management:

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

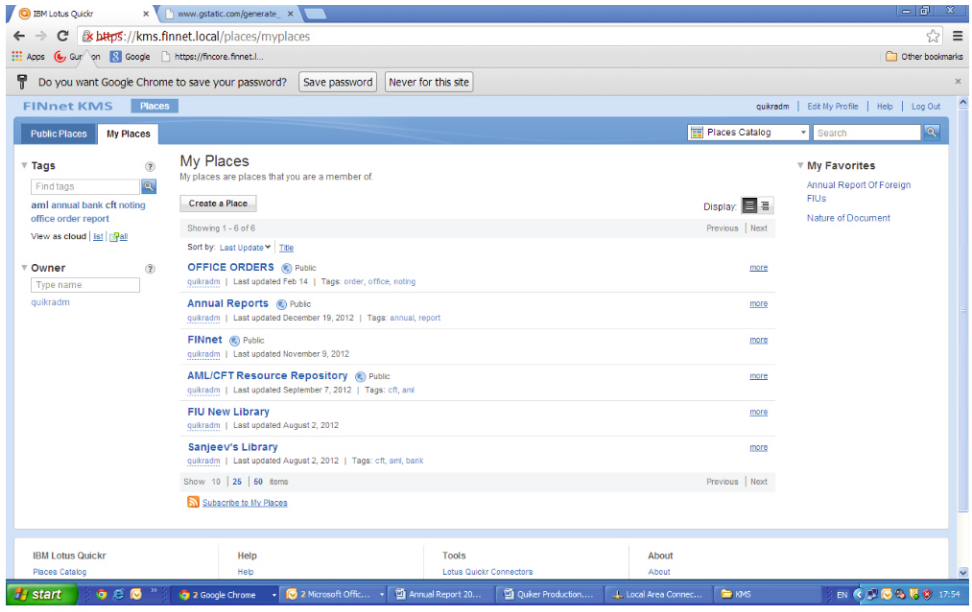


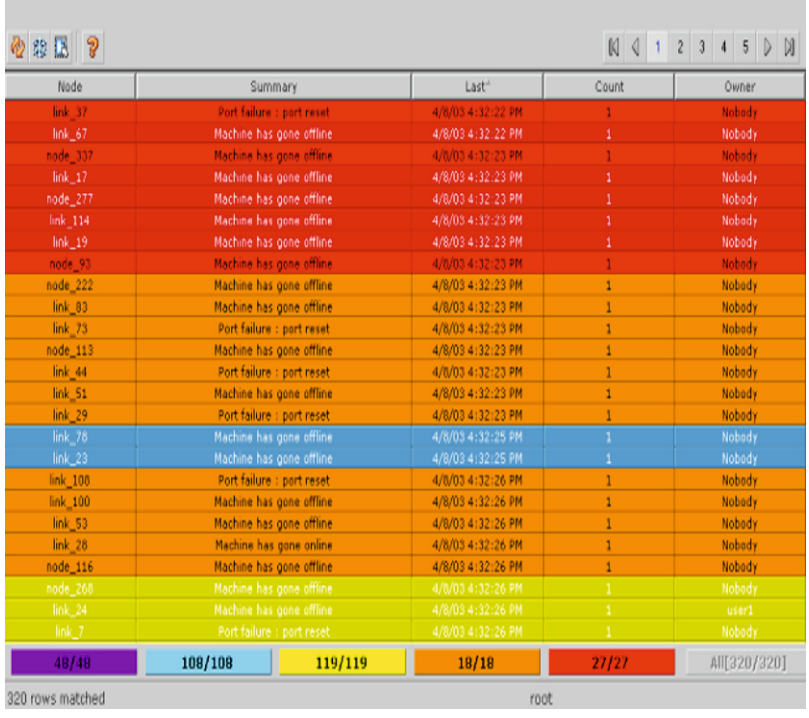
Figure for KMS

Technical Infrastructure Management

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

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

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



Information Security Management

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

Future Challenges

FINnet has substantially enhances the efficiency and effectiveness of FIU-IND's core function of collection, analysis and dissemination of financial information. IT enablement of key processes ensures higher productivity, faster turn around time and effective monitoring in all areas of FIU-IND's work. Current focus is to internalise the new reports introduced in PMLA amendment 2012 i.e. Cross Border Wire Transfer Report and Reports from Registrar and Sub registrar. System up gradation is also required to cater the needs of large volumes of reporting.

Appendix-A: Staff strength of FIU-IND

Post	**Sanctioned Strength**	**Working as on March 31, 2012**
Director	1	1
Additional Director / Joint Director	10	9
Technical Director	1	1
Joint Director Systems (earlier Principal System Analyst)	1	1
Deputy Director Systems	2	0
Deputy / Assistant Directors (earlier Senior Technical Officer)	21	15
Assistant Director Systems (earlier System Analyst/Programmer)	6	0
Group B, C & D	33	8
Total	**75**	**35***

* In addition 29 persons were working on contract basis.

Appendix-B : Chronology of Events for FIU-IND

2004-05	
Nov 18, 2004	Setting up of Financial intelligence unit- India (FIU-IND)
Mar 16, 2005	Appointment of First Director and FIU-IND becomes operational
2005-06	
Jul 1, 2005	PMLA and Rules thereunder brought into force
Mar 16, 2006	Launch of FIU-IND's website by the Hon'ble Finance Minister
2006-07	
Apr 3-5, 2006	On site visit of the Operational Working Group (OpWG) of theEgmont 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 NewDelhi
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 FINCEN, USA
Mar 26, 2010	Signed MoU with FIU of Sri Lanka
2010-11	
Apr 26-30,2010	Meeting with FATF Assessment Team at Sydney, Australia
May 5, 2010	Signed MOU with FIU of Georgia
June 10, 2010	Signed MOU with Financial IntelligenceAgency, San Marino
June 20-25, 2010	Attended third Plenary meeting of FATF XXI at Amsterdam, Netherlands
June 27- July 1,2010	Attended 18th Egmont Group Plenary at Cartagena, Columbia
July12- 16, 2010	Attended APG Annual Meeting at Singapore
Oct. 4 -7, 2010	Participated in Egmont Group/World Bank Tactical Analysis at Kuala Lumpur, Malaysia
Oct. 11 – 13, 2010	Attended Egmont Working Group and Committee Meetings at Chisinau, Moldova
Oct. 12, 2010	Signed MOU with Financial Intelligence Agency, Bermuda
Oct. 12, 2010	Signed MOU with Nigerian Financial Intelligence Unit, Nigeria
Oct. 18 – 22, 2010	Attended FATF Plenary at Paris, France
Oct. 25-28, 2010	Attended 2010 APG Typologies Workshop at Dhaka, Bangladesh
Nov. 8, 2001	Signed MOU with JapanFinancial Intelligence Centre, Japan

Nov. 15-19, 2010	Attended FATF/Egmont Group Joint Experts Meeting on ML/TF Typologies at Cape Town, South Africa
Dec. 6-10, 2010	Attended Regional Advanced Analysis Skills workshop at Kuala Lumpur
Jan. 25, 2011	Signed MOU with FINTRAC/PPATK, Indonesia
Feb. 21-25, 2011	Attended FATF Plenary at Paris, France
March 1, 2011	Attended ad-Hoc meeting on Financial Aspects of Piracy off the coast of Somalia at Washington, USA
Mar. 14-17, 2011	Attended Egmont Working Group (EWG) and Committee Meetings at Oranjestad, Aruba
Mar. 31, 2011	Phase I of Project FINnet completed
2011-12	
Apr 05-07, 2011	Attended regional workshop organized by AUSTRAC at Kathmandu, Nepal
Apr 21-22, 2011	Attended workshop organized by World Bank & EAG at Kiev, Ukraine
May 9-14, 2011	Attended training program on Prevention of Insurance Frauds at NIA, Pune
June 6-10, 2011	Attended training program organized by IMF at NIBM, Pune
June 14-17, 2011	Attended EAG Plenary & Working Group Meetings at Moscow, Russia
June 29, 2011	Attended 2nd Ad-hoc Meeting of Financial Aspect of Piracy at Seoul, South Korea
July 11-15, 2011	Attended training program organized by IMF at NIBM, Pune
July 11-15, 2011	Attended 19th Egmont Group Plenary at Yerevan, Armenia
July 12, 2011	Signed MoUs with FIUs of Israel and Poland
Aug. 22-25, 2011	Attended Analyst Exchange Program organized by FinCEN (US FIU) at Virginia, USA
Sept. 12-15, 2011	Attended Strategic Analysis Course organized by FIU, Qatar
Sept. 22-24, 2011	An officer visited FIU Mauritius to provide technical assistance and assessing their IT Infrastructure
Sept. 26-30, 2011	Attended FATF meeting at Rome, Italy
Oct. 7, 2011	Attended First Meeting of Working Group-5 of the Contact Group on Somali Piracy at Italy

Oct. 21-28, 2011	Attended FATF plenary at Paris
Oct. 24, 2011	Signed MoU with FIU, Singapore
Nov. 2-7, 2011	A team visited FIU Bhutan to provide technical assistancefor setting up FIU
Nov. 23-25, 2011	Attended 15th EAG plenary at Xiamen, China
Nov. 17, 2011	Signed MoU with Nepal
Dec. 9, 2011	Attended Joint APG/ Egmont Group FIU seminar at Busan, Korea
Jan. 30- Feb. 3, 2012	Attended EWG meetings at Manila, Philippines
Feb. 13-17,2012	Attended FATF Plenary and Working Group Meetings at Paris, France
Mar. 19-20, 2012	Attended 4th meeting of BIMSTEC at Bangkok, Thailand
Mar. 26, 2012	Phase II of Project FINnet completed
2012-13	
18 Apr 2012	An officer attended the FIU Forum of ESAAMLG at Arusha, Tanzania
16 - 20 Apr 2012	An officer attended the meetings of the sub-group of FATF on Effectiveness and Risk & Threat Assessment sub group
09 - 11 May 2012	An officer visited Bhutan as a member of APG team
18-20 June, 2012	An officer attended the Emerging Payment System Technical Capacity Building Workshop at Bangkok
18 - 22 Jun 2012	An officer attended FATF Plenary & it's Working Group Meeting at Rome, Italy
24 - 28 Jun 2012	An officer attended international conference on combating financial crimes at Dhaka, Bangladesh
28 Jun 2012	Director, FIU made a presentation on the AML/CFT framework of India and the role of its FIU in enhancing that framework at Mauritius
09 - 13 Jul 2012	Two officers attended the Egmont Charter Review Project Meeting and Egmont Plenary at St. Petersburg, Russia
9-13 July, 2012	Five officers attended a workshop on revised AML/CFT standards, organized by IMF, at Pune
9-14 July, 2012	Two officers attended a workshop on "BankingLaws & Fiscal Law Enforcement" at State Bank Staff College, Hyderabad
16 - 20 Jul 2012	An officer attended APG's 16th Annual Meeting and Technical Assistance Forum Meeting at Brisbane, Australia
10-14 Sept., 2012	Two officers attended a workshop on 'Investigating Economic Crimes in Financial Markets" at Mumbai
08-19 Oct., 2012	Three officers attended a workshop on "Intelligence gathering & intelligence tradecraft" at Gurgaon
30-31 Oct., 2012	Two officers attended a workshop on "Prevention ofsmuggling of FICN & Foreign Currency" at NACEN, Mumbai

09 Nov 2012	An officer attended the meeting of Working Group-5 of the Contact Group on Piracy off the Coast of Somalia (CGPCS) at Rome
26 - 28 Nov 2012	An officer participated in the meeting of FATF/GIABA Joint Experts Workshop on Money Laundering and Terrorist Financing Typologies at Senegal
14 - 17 Jan 2013	Two officers attended the Egmont Supervisory Course "Pilot" at Ottawa, Canada.
17-18 Jan., 2013	Two officers attended AML/CFT Workshop atNACEN, Mumbai
20 - 25 Jan 2013	Two officers attended the Egmont Working Group and Committee Meeting at Ostend, Belgium
08th Feb., 2013	Two officers attended a workshop on “Fraud in MLM, NTTS and CIS” at CBI Academy, Ghaziabad
18 - 22 Feb 2013	An officer attended the FATF Working Group and Plenary Meeting in Paris, France
06 - 07 Mar 2013	An officer attended the fifth BIMSTEC Sub Group Meeting on Combating the Financing of Terrorism at Dhaka, Bangladesh

Appendix C – Predicate offences under PMLA

PML (Amendment) Act, 2009 expanded the list of schedule offences under PMLA. PML(Amendment) Act 2012 removed the monetary threshold of Rupees 30 Lakh applicable to Part B offences by merging the offences of Part B in Part A. The list of offences (effective from 15th February 2013) is as under:

Part A of the Schedule: Offences under:

The Indian Penal Code,1860 (S.121 & 121A, S.489A & 489B)
The Narcotic Drugs & Psychotropic Substances Act, 1985 (S.15,16,17,18,19,20,21,22,23,24,25A, 27A & 29)
The Explosive Substances Act, 1908 (s.3, 4 & 5)
The Unlawful Activities (Prevention) Act, 1967 (S.10 read with S.3, S.11 read with S.3 & 7, S.13 read with S.3, S.16 read with S.15, S.16A,17,18,18A, 18B, 19, 20, 21, 38, 39 &40)
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 B of the schedule: Omitted by PML (Amendment) Act, 2012

Part C of the Schedule:

An offence which is the offence of cross border implications and is specified in Part A of the schedule or the 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 Preventon 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 thereof by the Adjudicating Authority.
01.07.2005	12/2005	Specified Rules relating to the manner of forwarding a copy of the order of retention of seized property along with the material to the Adjudicating Authority and its period of retention by the Adjudicating Authority.
01.07.2005	13/2005	Specified Rules for the manner of receiving the records authenticated outside India.
01.07.2005	14/2005	Specified Rules for the purpose of appeals under the Prevention of Money Laundering Act, 2002.
13.12.2005	15/2005	Amended Rules 5, 7, 8 and 10 of the Rules notified by Notification No. 9/2005
27.06.2006	6/2006	Specified the authorities to whom Director, FIU-IND can furnish information under Section 66 of the PMLA
24.05.2007	4/2007	Amended definition of suspicious transaction (Rule 2), counterfeit currency transaction [Rule 3(1)(C)], due dates for furnishing reports (Rule 8) and requirement of verification of the records of the identity of clients (Rule 9)
12.11.2009	13/2009	Amended Rule 2, 3, 5, 6,7, 8, 9 and 10 of the Rules notified by Notification No. 9/2005.
12.02.2010	67/2010	Amended requirements of maintenance of accounts and definition of beneficial owner.
16.06.2010	10/2010	Amended Rule 2,9,& 10 to include explanation to the definition of 'Suspicious Transaction' as transaction involving financing of activities related to terrorism, obligation to determine beneficial owner, ongoing due diligence, prohibition of keeping or opening anonymous or fictitious accounts, etc.
16.12.2010	14/2010	Amended Rule 2 & 9 to expand the list of 'officially valid documents' (Rule 2) by including letter issued by NREGA and Aadhar Number issued by UIDAI and inserted provisions to enable opening of 'small account'.
24.06.2011	6/2011	Amended the name of PMLA rule as notified vide Notification No 9/2005 to 'The Prevention of Money Laundering (Maintenance of Records) Rules,2005'.
27.8.2013	12/2013	Prevention of Money-laundering (Maintenance of Records) Amendment Rules, 2013 notified.

Appendix E : Important Circulars and 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 there under – Scheduled Commercial Banks*
3.03.2006	*PMLA- Obligation of banks in terms of Rules notified there under – 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 there under – Regional Rural Banks*
21.03.2006	*PMLA- Obligation of banks in terms of Rules notified there under – Primary Urban Co-operative Banks*
05.04.2006	*PMLA- Obligation of NBFCs in terms of Rules notified there under - 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 forall NBFCs, MNBs, RNBs*
01.07.2009	*Master Circular - Para-banking Activities for all scheduled commercial banks (excluding RRBs)*
01.07.2009	*Master Circular – Foreign Contribution (Regulation) Act, 1976*
01.07.2009	*Master Circular – KYC Guidelines – AML Standards for all NBFCs, MNBs, RNBs*
19.11.2009	*KYC norms/ AML standards/CFT- Obligation of Authorised Persons - Money changing activities*
11.08.2009	*List of Terrorist Individuals/Organisations- under UNSCR 1267(1999) and 1822(2008)*
14.08.2009	*Use of RTGS/NEFT/NECS/ECS- Compliance with FEMA Regulations and Wire Transfer Guidelines*
14.08.2009	*Policy Guidelines for issuance and operation of Prepaid Payment Instruments in India*
27.11.2009	*KYC norms/ AML standards/CFT- Cross Border Inward Remittance under MTSS*
11.09.2009	*KYC norms / AML standards/CFT/Obligation of scheduled commercial banks*
16.09.2009	*Adherence to KYC/AML guidelinesMulti Level Marketing firms - Primary (Urban) Co-operative Banks*
17.09.2009	*CFT - Unlawful Activities (Prevention) Act, 1967– Obligation of scheduled commercial banks*
29.09.2009	*KYC Norms / AML Standards and obligation of Regional Rural Banks (RRBs)*
30.09.2009	*KYC / AML Standards / CFT / Obligation of State and Central Co-operative Banks*
29.10.2009	*CFT- Unlawful Activities (Prevention) Act, 1967– Obligation of State and Central Co-operative Banks*
05.11.2009	*CFT- Unlawful Activities (Prevention) Act, 1967– Obligation of RRBs*

13.11.2009	Prevention of Money Laundering Act, 2002 – Obligation of Urban Co-operative Banks (UCBs)
13.11.2009	KYC Norms/AML Standards/CFT/Obligations under PMLA 2002- NBFCs
16.11.2009	CFT- Unlawful Activities (Prevention) Act, 1967– Obligation of UCBs
16.11.2009	KYC Norms/AML Standards/CFT/Obligations under PMLA 2002- UCBs
27.11.2009	KYC norms/ AML standards/CFT- Obligation of Authorised Persons- Money changing activities
22.12.2009	KYC norms/ AML standards/CFT- Obligation of Payment System Operators
12.01.2010	Prevention of Money-laundering Amendment Rules, 2009 - Obligation of banks/Financial Institutions
26.03.2010	KYC guidelines- accounts of proprietary concerns - Obligation of Scheduled Commercial Banks
26.03.2010	KYC norms/AML Standards/CFT/Obligation of Scheduled Commercial Banks
Apr – May, 2011	Anti-Money Laundering (AML) /Combating of Financing Terrorism (CFT) Standards. FATF Statement identifying a list of jurisdictions which have strategic AML/CFT deficiencies to Authorized Persons, MTSS, PSO, DCCBs,StCBs, Money Changing Activities, UCBs, NBFCs, RNBCs.
05.04. 2011	Operation of deposit accounts with NBFCs and money mules.
01.07.2011	Master Circular on Money Transfer Service Scheme.
01.07.2011	Master Circular on Know Your Customer (KYC) Norms/ Anti-Money Laundering (AML) Standards/ Combating of Financing of Terrorism (CFT) Obligation of banks under Prevention of Money Laundering Act, 2002. to All Scheduled Commercial Banks (Excluding RRBs)/ All India Financial Institutions/ Local Area Banks. UCBs
01.07.2011	Master Circular – KYC Guidelines- Anti-Money Laundering Standards – PMLA, 2002– Obligations of NBFCs.
08.08.2011	Opening of "Small Account"
02.10.2011	Appointment of Agents/ Franchisees by Authorized Dealer Category – I banks, Authorized Dealer Category – II and Full Fledged Money Changers– Revised guidelines.
09.11.2011	UCBs – KYC Norms– Letter issued by UDAI containing details of name, address and Aadhaar number.
22.12.2011	KYC Norms/ AML Standards/CFT– Obligation of Authorized Persons under PMLA, 2002
30.12.2011	KYC Norms /AML Standards/CFT/Obligation of Banks under PMLA 2002-Assessment and Monitoring of Risk.
12.01.2012	Anti -Money Laundering / CFT standards
16.01.2012	RRBs - Anti Money Laundering / CFT Standards
16.01.2012	St. CBs / DCCBs– Anti Money Laundering / Combating Financing of Terrorism- Standards
09.02.2012	AML / CFT- Standards
15.02.2012	AML Standards / CFT Standards– Cross Border Inward Remittance under Money Transfer Service Scheme (MTSS)
15.02.2012	AML Standards / CFT Standards- Money Changing Activities
27.02.2012	AML / CFT Standards– Primary (Urban) Cooperative Banks
29.02.2012	KYC Norms / AML Standards / CFT / Obligation of Authorised Person under PMLA, 2012, Assesment and monitoring and Risk – Money Changing Activities
05.03.2012	UCBs – KYC Norms / AML Standards / CFT Standards / obligations of banks under PMLA, 2012-Assesment & Monitoring of Risk
14.03.2012	AML / CFT- Standards
15.03.2012	RRBs / St. CBs / DCCBs- AML / CFT Standards
21.03.2012	NBFCs– KYC Norms / AML Standards / CFT / Obligations of banks under PMLA 2002-Assesment and Monitoring of Risk
04.04.2012	AML/ CFT Standards
11.04.2012	AML / CFT Standards
17.04.2012	AML / CFT Standards- Cross border Inward Remittances under MTSS
	AML / CFT Standards– Money Changing Activities
	KYC Guidelines- According of proprietary concerns
18.04.2012	St CBs / DCCBs- KYC Guidelines- Accounts of proprietary concerns
11.05.2012	KYC Guidelines- Accounts of Proprietary concerns
29.05.2012	KYC Guidelines- Accounts of Proprietary concerns
08.06.2012	KYC / AML / CFT- Risk Categorization & Uploading of Customer Profiles
11.06.2012	KYC / AML / CFT- Risk Categorization & Uploading of Customer Profiles
08.06.2012	KYC / AML / CFT Guidelines Unique customer identification code (UCIC) for banks customers in India
11.06.2012	KYC / AML / CFT Guidelines - Unique customer identification code (UCIC) for banks customers in India
02.07.2012	Master Circular - KYC Norms / AML Standards / CFT / obligation of banks under PMLA, 2012
02.07.2012	Master Circular - KYC Norms / AML Standards / CFT / obligation of banks under PMLA, 2012– Obligation of NBFCs in terms of rules notified thereunder
26.07.2012	KYC Norms / AML Standards / CFT- Risk categorization and updation of customer profiles
27.07.2012	AML / CFT Standards

03.08.2012	UCBs - AML / CFT Standards
23.08.2012	AML/ CFT Standards – Cross border Inward Remittance under MTSS AML / CFT Standards Money Changing Activities
13.09.2012	KYC / AML / CFT- Risk Categorisation and updation of customer profiles- Primary UCBs
17.09.2012	NBFCs /RNBCs- AML / CFT Standards
24.09.2012	KYC Norms / AML Standards / CFT obligation of Authorised Persons under PMLA, 2012, as amended by PMLA Amendment Act, 2009- Money Changing Activities
09.10.2012	KYC / AML / CFT Guidelines UCK code- Primary UCBs
15.11.2012	KYC / AML Standards / CFT / obligations of Authorised persons under PMLA
10.12.2012	KYC Norms / AML standards / CFT standards / obligations of banks and PMLA, 2012
12.12.2012	AML / CFT Standards
13.12.2012	AML/ CFT / Obligation of Banks under PMLA, 2012
19.12.2012	AML/ CFT / Obligation of Banks under PMLA, 2012
28.12.2012	AML/ CFT / Obligation of Banks under PMLA, 2012
02.01.2013	KYC Norms / AML Standards / CFT / Obligations of Authorised persons under PMLA, 2012 as amended by Prevention of Money Laundering (Amdt.) Act, 2009 - Money Changing Activities
02.01.2013	KYC Norms / AML Standards / CFT / Obligations of Authorised persons under PMLA, 2012 as amended by Prevention of Money Laundering (Amdt.) Act, 2009– Cross Border Inward Remittance under MTSS
10.01.2013	AML / CFT standards- Cross border Inward Remittance under MTSS
10.01.2013	AML / CFT standards- Money Changing Activities
18.01.2013	KYC Norms / AML / CFT standards / Obligation of banks under PMLA, 2012
22.01.2013	KYC Norms /AML / CFT standards / Obligation of banks under PMLA, 2012
28.01.201	KYC Norms / AML / CFT standards / Obligation of banks under PMLA, 2012
29.01.2013	KYC Norms / AML / CFT standards / Obligation of banks under PMLA, 2012
31.01.2013	RRBs / St. CBs / DCCBs - KYC Norms / AML / CFT Obligation of Cross border bank under PMLA, 2012
22.02.2013	KYC Norms / AML standards / CFT standards Obligation of Authorised persons under PMLA, 2002
07.03.2013	KYC Norms / AML Measures / CFT / Obligation of Banks under PMLA 2002– Primary UCBs

Securities Exchange Board of India (SEBI)	
18.01.2006	Guidelines for Anti Money Laundering Measures
20.03.2006	Obligations of Intermediaries under the PMLA
27.04.2007	Permanent Account Number (PAN) to be the sole identification number
19.12.2008	Master Circular on AML/CFT obligations of Securities Market Intermediaries
01.09.2009	AML Standards/CFT/Obligations of Securities Market Intermediaries
23.10.2009	CFT under Unlawful Activities (Prevention) Act, 1967– all registered intermediaries
14.06.2010	AML Standards / CFT-Obligation of Securities Market Intermediaries
05.10.2011	Uniform Know Your Client (KYC) requirements for the securities market.
25.10.2011	In-person verification (IPV) of clients by subsidiaries of Stock Exchanges, acting as Stock Brokers
02.12.2011	The Securities and Exchange Board of India (KYC Registration Agency) Regulations, 2011
23.12.2011	Guidelines in pursuance of the SEBI KYC Registration Agency (KRA) Regulations, 2011 and In-Person Verification (IPV)
13.04.2012	Uploading of the existing clients KYC details in the KYC Registration Agency (KRA) system by the intermediaries
13.08.2012	Aadhar letter as proof of address for KYC norms
05.09.2012	KYC requirements
28.03.2013	Amendments of SEBI (KYC Registration Agency) regulations, 2011 and relevant circulars

Insurance Regulatory and Development Authority (IRDA)	
31.03.2006	Guidelines of Anti Money Laundering Programme for Insurers
24.11.2008	Master Circular on AML/CFT obligations of Insurance Companies
18.08.2009	Requirement of PAN for Insurance Products for Insurers
24.08.2009	AML Guidelines for Insurance Companies
13.05.2010	Prevention of Money-laundering Amendment Rules, 2010- Obligation of Insurers
16.06.2010	Anti Money Laundering Guidelines- Obligation of Insurers
28.10.2009	Guidelines for implementation of Section 51A of Unlawful Activities (Prevention) Amendment Act
09.09.2009	The Prevention of Money Laundering (Amendment) Act, 2009 for Insurance Companies

05.07.2011	Amendment to Rule 2(d) of PML (Maintenance of Records) Rules, 2005
05.10.2011	AML/CFT Guidelines– Cash Acceptance Threshold
01.01.2012	Amendment of clause 3.1.1(xiv) of the Master Circular 2010 on AML/CFT guidelines on conducting detailed due diligence while taking insurance risk exposure to individuals/ entities connected with countries identified by FATF as having deficiencies in their AML/CFT regime.
27.01.2012	AML / CFT Guidelines
28.12.2012	AML / CFT Guidelines
05.02.2013	AML / CFT Guidelines–Procedure for Determination of Beneficial Ownership

National Housing Bank (NHB)	
31.03.2005	KYC Guidelines- Identification of customers- for Housing Finance Companies
10.04.2006	KYC Guidelines / AML Standards for Housing Finance Companies
17.01.2007	KYC Guidelines / AML Standards-Reporting System for Housing Finance Companies
25.07.2007	KYC Guidelines / AML Standards-Reporting System for Housing Finance Companies
20.02.2009	KYC Norms/AML Standards / Combating of Financing of Terrorism (CFT) for Housing Finance Companies
23.06.2009	KYC Norms/AML Standards / Combating of Financing of Terrorism (CFT) for Housing Finance Companies
25.01. 2010	`Know Your Customer (KYC) Norms/ Anti-Money Laundering (AML) Standards/ Combating of Financing of Terrorism (CFT)
06.05.2011	Guidelines on "Know Your Customer"& Anti-Money Laundering Measures" for HFCs

Appendix F : Obligations of Reporting Entities under PMLA

Obligation	When
Communicate the name, designation and address of the Designated Director and Principal Officer to FIU-IND	At the time of appointment/ change of Designated Director and Principal Officer
Formulate and implement a Client Due Diligence(CDD) Programme to determine true identity of clients	Initially and in pursuance of any change being prescribed by the Regulator
Identify the client, verify their identity and obtain information on the purpose and intended nature of the relationship	At the time of commencement of account-based relationship
Verify the identity of the client	At the time of carrying out a transaction for an amount equal to or exceeding Rupees fifty thousand or any international money transfer operation
Determine whether a client is acting on behalf of a beneficial owner and identify the beneficial owner and take all steps to verify the identity of the beneficial owner	At the time of commencement of the relationship and at the time of any change in beneficiary/ authorized person
Obtain a certified copy of documents in evidence of identity and address and a recent photograph and other documents in respect of the nature of business and financial status of the client (as may be prescribed by the Regulator)	At the time of commencement of account-based relationship
Evolve internal mechanism for maintaining and furnishing information	Ongoing
Maintain record of all transactions that allows reconstruction of individual transactions including the nature of transaction, the amount and currency of transaction, the date of the transaction and the parties of the transaction	Ongoing
Examine transactions and to ensure that they are consistent with the business and risk profile of the customer	As an ongoing due diligence
Furnish Cash Transaction Report (CTR) to FIU-IND containing specified cash transactions	Within 15th day of succeeding month (Monthly Reporting)
Furnish Counterfeit Currency Report (CCR) to FIU-IND Furnish report in respect of Non-Profit-Organizations (NPOs)	Within 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.
Furnish Electronic Fund Transfer Report to FIU-IND containing specified cross border transactions	Within 15th day of succeeding month (Monthly Reporting)
Furnish Report on Registration of Properties to FIU-IND (by Registrar and Sub-Registrar of Properties)	Every Quarter by 15th day of the month succeeding the quarter
Maintain records of identity of clients	For a period of 5 years after the business relationship between a client and the reporting entity has ended or the account has been closed whichever is later.
Maintain records of all transactions	For a period of 5 years from the date of transaction between a client and the reporting entity
Keep the information maintained, furnished or verified confidential	Ongoing

Appendix G : Interaction with partner agencies

April-12	• Directorate of Vigilance & Anti-Corruption, T.N.	• Role of FIU
May-12	• The Indian Institute of Management	• Lecture on 'Anti Money Laundering' during the Mid-career Training Programme
July-12	• NADT Nagpur	• Role of FIU in Investigating Tax Offences
	• NADT Nagpur	• Overview of FIU-IND-role & function
	• IIM, Bangalore	• Role of FIU-IND
	• NACEN Delhi	• FATF-AML/CFT Regime in India
Aug-12	• NIA	• Terror Funding and FICN Circulation
	• National Police Academy	• AML/CFT regime and role of FIU
	• The National Academy of Customs, Excise and Narcotics Faridabad	• Role of FIU-IND
Sep-12	• FIU-IND	• Risk Based Approach and NMTRA Report
	• CBI Academy	• Introduction to Collection of Criminal Intelligence in PMLA and Overview of FIU-IND & its Role
Oct-12	• MDSET	• Workshop on FICN
Nov-12	• FIU-IND	• Workshop on FINex
Dec-12	• FIU-IND	• FINex Workshop
	• Regional Economic Intelligence council, Delhi	• FINex
	• DGCEI	• FINex
	• IB	• FINex
	• FIU-IND	• FINex

Jan-13	• NCB	• Role and function of FIU-IND in Financial Investigation
	• RTI, Direct Taxes	• Role and function of FIU-IND
	• FIU-IND	• FINex Workshop
Feb-13	• NACEN, Faridabad	• Role and functions of FIU-IND
	• Enforcement Directorate	• FIU & its working
Mar-13	• Chattisgarh Police	• Financial Frauds
	• CBDT	• FINex users orientation
	• IGP, Chandigarh (UT)	• AML/CFT regime, functioning of FIU - Coordination with LEAs/EOW of Police, amendments to PMLA/UAPA
	• IGP, Chandigarh (UT)	• AML/CFT regime, functioning of FIU - Coordination with LEAs/EOW of Police, amendments to PMLA/UAPA
	• NIA	• Role and functions of FIU-IND
	• IGP, Chandigarh (UT)	• AML/CFT regime, functioning of FIU - Coordination with LEAs/EOW of Police, amendments to PMLA/UAPA
	• West Bengal Police HQrs	• Meeting with West Bengal Police

Appendix H – Important FATF recommendations pertaining to Financial Intelligence Units

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

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

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

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

Interpretive Note

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

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

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

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

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

Recommendation 10 (Customer due diligence)

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

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

(i) establishing business relations;

(ii) carrying out occasional transactions: (i) above the applicable designated threshold

(USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the

Interpretive Note to Recommendation 16;

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

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

The CDD measures to be taken are as follows:

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

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

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

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

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

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

Interpretive Note

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

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

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

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

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

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

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

(a) Customer risk factors:

☐ The business relationship is conducted in unusual circumstances (e.g. significant unexplained

geographic distance between the financial institution and the customer).

☐ Non-resident customers.

☐ Legal persons or arrangements that are personal asset-holding vehicles.

☐ Companies that have nominee shareholders or shares in bearer form.

☐ Business that are cash-intensive.

☐ The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

(b) Country or geographic risk factors:

☐ Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.

☐ Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.

☐ Countries identified by credible sources as having significant levels of corruption or other criminal activity.

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

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

☐ Private banking.

☐ Anonymous transactions (which may include cash).

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

☐ Payment received from unknown or un-associated third parties

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

- Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

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

Examples of possible measures under simplified CDD are:

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

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

Recommendation 11 (Record-keeping)

Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

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

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

Recommendation 12 (Politically exposed persons)

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

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

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

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

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

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

Interpretive Note

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

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

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

Recommendation 15 (New technologies)

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

Recommendation 16 (Wire transfers)

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

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

Recommendation 17 (Reliance on third parties)

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

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

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

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

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

Recommendation 18 (Internal controls and foreign branches and subsidiaries)

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

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

Interpretive Note

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

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

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

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

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

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

Recommendation 20 (Reporting of suspicious transactions)

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

Interpretive Note

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

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

Recommendation 21 (Tipping-off and confidentiality)

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

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

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

Recommendation 22and 23(DNFBPs: Customer due diligence)

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

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

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

Countries should take measures to prevent the misuse of legal persons and arrangements for money laundering or terrorist financing. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons or express trusts (including information on the settlor, trustee and beneficiaries) that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares or bearer share warrants, or which allow nominee shareholders or nominee directors, should take effective measures to ensure that they are not misused for money laundering or terrorist financing. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22.

Interpretive Note

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

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

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

(c) make the above information publicly available; and

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

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

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

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

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

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

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

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

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

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

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

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

Supervisors should have adequate powers to supervise or monitor, and ensure compliance by, financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial

institutions that is relevant to monitoring such compliance, and to impose sanctions, in line with Recommendation 35, for failure to comply with such requirements.

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

Interpretive Note

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

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

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

Recommendations 29 (Financial Intelligence Units)

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

Interpretive Note

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

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

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

29.4 In addition to the information that entities report to the FIU (under the receipt function), the FIU should

be able to obtain and use additional information from reporting entities as needed to perform its analysis properly.

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

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

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

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

Recommendations 34 (Guidance and feedback)

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

Recommendations 35 (Sanctions)

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

Recommendations 40 (Other forms of international co-operation)

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

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

Interpretive Note

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

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

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

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

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

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

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

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

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

Rec. No.	Recommendation	Rating
	Legal System	
1	Criminalization of money laundering offence	PC
2	Money laundering offence- mental element and corporate liability	LC
3	Confiscation and provisional measures	PC
	Preventive measures	
4	Secrecy laws consistent with the Recommendations	C
5	Customer Due Diligence	PC
6	Politically Exposed Persons	PC
7	Correspondent banking	LC
8	New technologies and non face-to-face business	LC
9	Third parties and introducers	N/A
10	Record keeping	LC
11	Unusual transactions	LC
12	Designated Non-Financial Businesses and Professions (DNFBPs)	NC
13	Suspicious transaction reporting	PC
14	Protection and no tipping off	LC
15	Internal controls, compliance and audit	LC
16	Application of R 13,15 and 21 to DNFBPs	NC
17	Effective, proportionate and dissuasive sanctions	PC
18	Operation of Shell Banks	LC
19	Other forms of reporting	C
20	Other NFBP and secure transaction techniques	LC

21	Special attention to higher risk countries	PC
22	Foreign branches and subsidiaries	C
23	Regulation supervisions and monitoring	PC
24	DNFBP- Regulation supervisions and monitoring	NC
25	Guidelines and feedback	LC
	Institutional and other measures	
26	Financial Intelligence Unit	LC
27	Law enforcement authorities	LC
28	Powers of competent authorities	C
29	Powers of supervisors	LC
30	Resources, integrity and training	LC
31	Co-operation among national agencies	LC
32	Maintenance of comprehensive statistics	LC
33	Unlawful use of legal persons	PC
34	Unlawful use of legal arrangements	PC
	International Co-operation	
35	Implementation of international conventions	PC
36	Mutual Legal Assistance and extradition	LC
37	Dual criminality	LC
38	Mutual Legal Assistance on confiscation and freezing	LC
39	Money laundering as extraditable offence	LC
40	Other forms of co-operation	LC

FATF Special Recommendations on Terrorist Financing

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

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

Note: In the 8th Follow-up Report of the Mutual Evaluation of India, the FATF has observed that overall; India has reached a satisfactory level of compliance with all of the core and key Recommendations. The mutual evaluation follow-up procedures indicate that India has made sufficient progress for all core and key Recommendations. Consequently, it was recommended that India be removed from the regular follow-up process. The report was accepted by the Plenary of FATF in its June 2013 session at Oslo, Norway.

For full report of the FATF, please check the link below:

http://www.fatf-gafi.org/media/fatf/documents/reports/mer/India_FUR8_2013.pdf

Appendix J–Outreach

April-12	• Awareness of obligations under PMLA, Chennai
May-12	• Review of Compliance to PMLA, 2002, Mumbai • Review of Compliance to PMLA, 2002, Mumbai • AML-CFT Regime Obligations under PMLA, 2002, Ahmedabad • AML-CFT Regime Obligations under PMLA, 2002, Ahmedabad
June-12	• AML-CFT Regime Obligations under PMLA 2002, Rajkot • AML-CFT Regime Obligations under PMLA 2002, Rajkot • Compliance Issues, Kolkata • Review Meeting of Compliance of PMLA, Kolkata • AML / CFT Regime, Thrissur, Kerala • (1) International AML/CFT Standards and AML/CFT Regime in India / (2) Addressing the Risk of Money Laundering & TF, Mumbai
July-12	• Review of AML/CFT compliance of UCB's, Mount Abu • AML/CFT Compliance, Mumbai • Review of AML/CFT compliance of UCB's, Raipur • Review of AML/CFT compliance of UCB's, Mumbai
Aug-12	• Review & Training Program on AML/CFT, Karad • Review & Training Program on AML/CFT, Karad • Review & Training Program on AML/CFT, Kolhapore • Review & Training Program on AML/CFT, Kolhapore • Review & Training Program on AML/CFT, Karad • Review & Training Program on AML/CFT, Karad • Review of Training on AML/CFT, Hyderabad • Review of Training on AML/CFT, Hyderabad
Sep-12	• 'AML/CFT Regime in India, Role of FIU-IND & Obligations of Reporting Entity', SBI Academy Gurgaon • Risk Based Approach and NMTRA Report, New Delhi • AML/CFT, PMLA, Role of FIU-IND Obligations of Reporting Entities, New Delhi

Oct-12	• Project FINnet Implementation of Red Flag IndicatorsUploading of Reports, Mumbai • Review of the compliance of UCBs to AML/CFT regime, Kochi • Review of the compliance of UCBs to AML/CFT regime, Kochi • Review of the compliance of UCBs to AML/CFT regime, Kochi • Review of the compliance of UCBs to AML/CFT regime, Kochi • Train the Trainer Workshop on AML/CFT/KYC, New Delhi • Project FINnet Uploading of Reports, New Delhi • Project FINnet Uploading of Reports, Mumbai • Project FINnet Uploading of Reports, Mumbai • PMLA, Delhi • PMLA, Delhi • Issues relating to STRs, Mumbai • Issues relating to STRs, Mumbai • Issues relating to STRs, Mumbai
Nov-12	• Review of Private Foreign Banks, Mumbai • Technology to meet Regulatory Expectations, Mumbai • FINnet Registration / upload of reports, New Delhi • FINnet Registration / upload of reports, New Delhi
Dec-12	• Registeration/Upload of Reports on FINnet Gateway, Ahmedabad • Registeration/Upload of Reports on FINnet Gateway, Mumbai • Inaugauration of KYC/AML workshop and interface session with DMLRDs, Jaipur • Review of AML/CFT related issues, Mumbai
Jan-13	• Uploading of Reports on FINnet Gateway, Karad • Obligation of Banks, Uploading of Reports on FINnet Gateway, PMLA amendments, Mumbai
Feb-13	• Information to be furnished to FIU-IND & records to be maintained, Pune • KYC/AML regime and obligations of Coop. Sector Banks, Pune • Uploading of reports on FINnet Gateway, PMLA Amendments, Hyderabad
Mar-12	• Efforts against ML & related crimes, efiling of reports, Pune • AML/CFT regulations etc., New Delhi • Closing address in the AML / CFT seminar, Mumbai • Panel discussion on sanctions and Anti Bribery & Corruption measures, AML Surveillance & STR sharing,Mumbai • Implementation of KYC/AML/CFT measures etc., Mumbai • E-filing of reports, AML/CFT role of FIU & obligations of REs, New Delhi • Addressing the Risk of ML and TF in stock market, Kolkata • Implementation of AML/CFT Regime, Chennai • AML / CFT regime underPMLA, 2002, Chennai

Glossary:

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

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

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

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

Website :
http://fiuindia.gov.in

E-mail :
helpdesk@fiuindia.gov.in **(helpdesk for Project FINnet Gateway Portal)**
ctrcell@fiuindia.gov.in **(for queries on CTR data quality)**
feedbk@fiuindia.gov.in **(for feedback)**