Annual Report 2013-14

Financial Intelligence Unit-India

Ministry of Finance, Government of India

सत्यमेव जयते

Annual Report
2013-14

Department of Revenue
Ministry of Finance, Government of India

अरुण जेटली
वित्त, कार्पोरेट कार्य
एवं रक्षा मंत्री
भारत

सत्यमेव जयते

Arun Jaitley
Minister of Finnance,
Corporate Affairs
and Defence
India

MESSAGE

I am glad to know that Financial Intelligence Unit-India (FIU-IND) is coming out with its 7th Annual Report for the year 2013-14. Since it was set-up in 2004, FIU-IND has come a long way in establishing itself as the national center for receipt, analysis and dissemination of financial intelligence relating to money-laundering, terrorist financing and associated crimes.

Financial crimes are increasingly becoming more sophisticated and often have cross-border connections. Accordingly, in addition to domestic inter-agency co-operation, international co-operation is critical for successful investigation of financial crimes. FIU-IND has to play a pivotal role in ensuring transfer of intelligence from the financial sector to the domestic law enforcement agencies on the one hand and in coordinating the exchange of information with foreign FIUs on the other.

I am happy to learn that FIU-IND has effectively integrated information technology in the performance of its core functions of receipt, analysis and dissemination making the process of information management more organized and efficient. I hope that FIU-IND keeps assessing and upgrading its technological capabilities periodically and employ cutting edge technology to perform its functions effectively.

FIU-IND needs to be focus on some significant challenges arising out of the changing international AML/CFT regime. These include playing a more proactive role in the international cooperation for exchange of information, enhancing the capacities of the reporting entities to furnish high quality STRs, outreach to new reporting entities and ensuring compliance with the PMLA. Enhanced coordination with the domestic agencies, including revenue collecting authorities, and improved access to administrative, financial and law enforcement databases, is another area that FIU needs to focus on in order to increase the overall effectiveness of the regime.

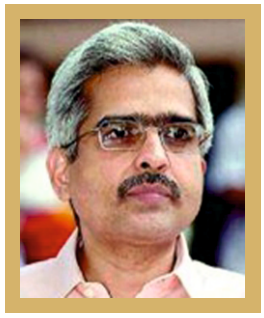
I convey my best wishes to the officers and staff of FIU-IND.

(Arun Jaitley)

शक्तिकान्त दास, आई.ए.एस.
राजस्व सचिव
SHAKTIKANTA DAS, I.A.S.
Revenue Secretary
Tel. : +91-11-23092653
Fax : +91-11-23092719
E-mail : rsec@nic.in
website : www.finmin.nic.in

सत्यमेव जयते

भारत सरकार
वित्त मंत्रालय
राजस्व विभाग
नॉर्थ ब्लॉक,नई दिल्ली-110001
Government of India
Ministry Finance
Department of Revenue
North Block, New Delhi-110001



MESSAGE

The Financial Intelligence Unit-India (FIU-IND) has been assigned a key role under the Prevention of Money Laundering Act 2002 (PMLA). Its roles and responsibilities relate to receipt, analysis and dissemination of information in accordance with the international standards set by the Financial Action Task Force (FATF) and the Egmont Group of FIUs.

The volume of information handled by FIU-IND has been growing continuously over the years. By the end of 2013-14, FIU-IND has received more than 50 million cash transaction reports and over 1,60,000 suspicious transaction reports. FIU-IND has harnessed information technology to handle the increasingly larger number of reports and to carry out operational as well as strategic analysis of the suspected proceeds of crime. The role of FIU-IND in providing critical intelligence input to law enforcement agencies will significantly depend on the capacity of FIU to handle information quickly and efficiently.

With the introduction of the amendments to the Prevention of Money Laundering Act (PMLA) in 2013, the canvas of reporting entities has enlarged. Introduction of a new report on cross border wire transfers will provide FIU useful information in the analysis of financial crimes with cross-border connections. The amended PMLA has given FIU the power of calling for additional information from reporting entities and applying a range of sanctions for non compliance.

I am happy to observe that FIU-IND has also been making contributions to international forums like the Egmont Group of FIUs. FIU-IND has actively participated in the revision of the Egmont Charter and its follow-up works. FIU-IND is encouraged to contribute to the National ML & TF Risk Assessment in preparation for the next mutual evaluation by the FATF.

I wish the officers and staff of FIU-IND success in their endeavors.

(Shaktikanta Das)

Director's Report

Director's Report

The year 2013-14 has been a significant year for the FIU-India. During the year FIU-IND met with its most significant challenge, that is, to stabilise the FINnet, which is FIU-IND's integrated online system of receiving, processing, analysing and disseminating information that was commissioned in February 2013. FIU receives online statutory filings from thousands of reporting entities comprising banks, insurance companies, capital market intermediaries, non-banking finance companies, payment system operators, money remitters etc. These filing comprise both threshold based reports (Cash Transaction Reports, averaging 7-8,00,000 per month; and Non Profit Organisations Transaction Reports); and incident based reports, such as Counterfeit Currency Report (over 25,000 reports per month) and the Suspicious Transaction Reports (STR), averaging over 5,000 reports per month. These reports are filed through FINnet's FINgate platform in encrypted mode. FINgate is also used by FIU to communicate with the reporting entities through a secure, electronic medium that ensures speed and efficiency. The system also has the facility to send SMS to the principal officers of the reporting entities in situations that require immediate attention.

FINnet's core processing system, FINcore, uses business intelligence (BI) tools, to help FIU perform operational (targeting entities requiring investigation) and strategic analysis (analysis of trends and patterns). Stabilising the FINcore presented major challenges during the year, both because of the quality of the legacy data received in FIU since inception (2005-6), and the complexity of the operations involved. With sheer dedication, the FIU team, together with the System Integrator, was able to resolve the numerous issues of the FINcore, which now presents a state-of-the-art solution to FIU operations that only a few FIUs have been able to implement.

Another milestone for the year 2013-14 has been the introduction of a new report on cross border transactions of more than rupees five lakh or its equivalent in foreign currency. FIU was able to successfully carry out modifications in FINgate to enable the reporting entities to file the Cross Border Wire Transfer Reports (CBTR) on a monthly basis. FIU-India is one of the few FIUs in the world to have implemented this report, which has the potential to play an important role in the analysis of Illicit Financial Flows (IFF). Several studies, including those by the OECD, indicate that the developing countries lose hundreds of millions of dollars every year through illicit flows, including through trade mis-invoicing. It is hoped that the analysis of CBTR data will help in analysing the problem of IFF from India.

The effectiveness of an FIU is greatly enhanced by the capability of its reporting entities to generate quality STRs. To this end, FIU-IND attaches considerable importance to its outreach

activities, which include training the reporting entities, developing red flag indicators for different sectors, and sensitising the reporting entities about the emerging trends and threats in money laundering and financing of terrorism. Following the 2013 amendment to the PML Act, which now places the responsibility of overall implementation of the PMLA obligations on the designated directors on the boards of the reporting entities. FIU undertook an extensive outreach programme in which more than 400 designated directors were addressed in various parts of the country. FIU's annual Train the Trainers event this year lasted for 2 days and witnessed a record number of 160 participants from the reporting entities.

FIUs are central to the international exchange of information on money laundering and financing of terrorism, as per the architecture approved by the FATF. The Egmont Group of FIUs, whose membership has now reached 147 countries, is now perhaps the most important platform for international exchange of information on AML/CFT. FIU-India has been actively participating in the activities of the Egmont Group, both at the policy and operational levels. As the Asia region representative on the Egmont Committee, FIU-India made important policy level interventions to promote the interests of the Asia Pacific region. Some of these interventions related to Egmont Group's decision making process and other governance issues including the governance of the information exchange process,and became the basis for some important amendments in the Egmont Charter. FIU-India has been canvassing for making the membership process more inclusive, considering that a large number of Asia Pacific region countries are not yet members of the Egmont Group, and for a sharper focus on Illicit Financial Flows that afflict the developing countries at large. FIU-India also contributed significantly to the development of an FIU Information System Maturity Model (FISMM) that has now been implemented by the Egmont Group.

During the year, FIU- India took concrete steps to monitor the feedback on the information disseminated to the law enforcement agencies. The feedback received during the year indicates that, based on the information received from FIU-India, unaccounted income detected by the agencies was of the order of Rs. 7,848 crore, while the amount of assets seized/frozen/confiscated was of the order of Rs. 195 crore. This is by no means a modest achievement, considering that feedback in a large number of cases is still awaited. FIU-India operated on modest budget of less than Rs. 23 crore in the year with a sanctioned strength of 75 officers and staff. FIU-India's highly motivated officers and staff will continue to work diligently to make FIU-India as one of the best in the world.

(P K Tiwari)
Director
Financial Intelligence Unit-India

Contents

Performance at a Glance : 2013-14

Collection of information

- Approx. 8.8 million Cash Transaction Reports (CTRs) received
- 61,953 Suspicious Transaction Reports (STRs) received
- 3,01,804 Counterfeit Currency Reports (CCRs) received
- 80,616 NPO Transaction Report (NTRs) received

Analysis and Dissemination of Information

- 35,696 STRs processed
- 15,288 STRs disseminated

Collaboration with domestic Law Enforcement and Intelligence Agencies

- Regular interaction and exchange of information
- Received 594 requests for information from Intelligence & Law Enforcement agencies
- Provided information in 567 cases requested by the agencies

Results of action on STRs

- CBDT detected unaccounted income of Rs.7,078 crore and seized assets of Rs.163 crore
- CBEC detected service tax evasion of Rs.750 crore and seized assets of Rs.17 crore
- ED detected proceeds if crime of Rs.20 crore and seized assets of Rs.15 crore
- ED registered 105 new ECIRs on the basis of FIU-IND information

Regional and global AML/CFT efforts

- 94 requests received from foreign FIUs
- 82 requests sent to foreign FIUs

Increasing awareness about money laundering and terrorist financing

- Contribution in 34 seminars and training workshops covering 2,447 participants
- Organized a 2-day 'Train the Trainer Programme' for AML/CFT capacity building with 160 participants from LEAs, Regulators and banks & financial institutions.

Improving compliance with the PMLA

- 25 review meetings held with Principal Officers.

Strengthening legislative and regulatory framework

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

Strengthening IT infrastructure

- Phase IV of the Project FINnet accepted. Maintenance phase commenced.
- Successful end-to-end flow of information implemented.
- Removal of bugs and introduction of user-friendly features.
- Proposal moved for Change Order to add new features and to integrate cross-border wire transfer reports.

Chapter 1

Financial Intelligence Unit – India

Financial Intelligence Units (FIUs) are national central agencies set up for for collecting, analysing and disseminating financial intelligence, particularly about suspicious financial transactions pertaining to money-laundering and financing of terrorism.

The FATF Recommendations, regarded as the international standards, have the following prescription on the Financial Intelligence Units (Recommendation 29):

> *"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.

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. The Office Memorandum states that FIU-IND will be an independent body reporting to the Economic Intelligence Council (EIC) headed by the Finance Minister. FIU-IND is under the administrative control of

Department of Revenue, Ministry of Finance. FIU-IND is an administrative FIU and 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 (Appendix A). The chronology of significant events for FIU-IND is at Appendix B.

As prescribed under the Prevention of Money Laundering Act (PMLA) and the rules framed thereunder, FIU-IND receives reports on cash transactions, suspicious transactions, counterfeit currency transactions, funds received by non-profit organisations and cross-border wire transfers above a specified threshold. These reports are filed by the reporting entities i.e. banks, financial institutions, capital market intermediaries and designated non-financial businesses and professions (DNFBPs). FIU-IND analyses the reports received and disseminates actionable intelligence to agencies specified in Section 66 of PMLA or notified thereunder. Two new reports have been introduced from 15th February 2013, one relating to cross border transactions and the other to immovable properties registered by Sub-registrars or Registrars of property. New reporting entities have also been brought under the PMLA including several DNFBPs.

Reports required to be filled under PMLA

- Cash Transaction Reports (CTR)
- Suspicious Transaction Reports (STR)
- Counterfeit Currency Report (CCR)
- NPO Report (NPR)
- Cross-border Wire Transfer Report
- Registration of Property Report (To be notified)

FIU-IND maintains a national database of financial transactions reported to it and shares this information with enforcement and intelligence agencies on request. FIU-IND also monitors and identifies strategic and key money laundering trends, typologies and developments based on the analysis of its database.

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 organization- 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

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

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

Chapter 2

Legal framework

Prevention of Money Laundering Act, 2002

The Prevention of Money Laundering Act, 2002 (PMLA) is India's legislation for combating money laundering. It was enacted in 2003 and brought into force on 1st July 2005. It criminalizes money laundering and provides for attachment, seizure and confiscation of property obtained or derived, directly or indirectly, from or involved in money laundering. The PMLA was brought into the statute 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 its financing.

Section 3 of PMLA, which criminalizes the activity of money laundering, reads 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 is a designated offence under the Narcotic Drugs and Psychotropic Substances Act, 1955. The property derived from or involved in money laundering is also liable for confiscation under PMLA.

The predicate offences 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 relating to maintenance and submission of information by the reporting entities to FIU and the second relating to investigations into cases of money laundering and powers of search, seizure, collection of evidence, prosecution, etc. The Director, FIU-IND is the relevant authority for enforcement of the provisions relating to maintenance of records and filing of information by the reporting entities. The Directorate of Enforcement is the relevant 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.

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 in 2005 and thereafter in 2009 and 2013 to overcome the difficulties being faced in its enforcement and to conform to the international standards. A comprehensive evaluation of the country's legislative and administrative framework for prevention of money laundering and countering the financing of terrorism was made by the FATF in November/December, 2009. 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 earlier 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 transactions 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:

The following financial sector entities have been brought under the 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 financial services

F. Inclusion of additional non-financial businesses and professions

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 agents,

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

d) Persons 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 when notified by the Central Government. The Central Government may 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 explicit powers have been given to the Director, FIU-IND to call for records of transactions or any additional information that may be required for the purpose of this Act.

b) separate sub-section has been included to put an obligation on the reporting entity to maintain confidentiality of the requests from FIU.

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.

Amendments to PML (Maintenance of Records) Rules 2005

The PML (Maintenance of Records) Rules, 2005 have also been amended to give effect to changes made in PMLA and revised recommendations of FATF. The salient features of the amendments are shown below:

a) Addition/modification in the definitions of:

(i) Client Due Diligence -Rule 2(1)(b)

(ii) Designated Director-Rule 2(1)(ba)

(iii) Officially Valid Documents -Rule 2(1)(d)

(iv) Regulator-Rule 2(1)(fa)

(v) Transaction-Rule 2(1)(h)

b) Clarification on Cash Transaction Report (series of cash transactions integrally connected) under Rule 3(1)(B)

c) Introduction of new reporting requirements on cross border transactions and registration of properties by registrar or sub-registrar under Rule 3(1)(E) & (F)

d) Monthly filing of counterfeit currency report and cross-border wire transfer report under Rule 8(1)

e) Registration of Property Report to be filed quarterly under Rule 8(3)

f) Delay in furnishing reports will be treated as violation under Rule 8(4)

g) Redrafting of Rule 9 to provide for:

(i) Verification of identity within reasonable time –Rule 9(1)(a)(ii)

(ii) Reliance on third party for CDD –Rule 9(2)

(iii) Rules for determination of Beneficial Ownership- Rule 9(3)

(iv) CDD for existing clients-Rule 9(12)(iii)

(v) Risk based approach (RBA) – Rule 9(13)

(vi) Regulators to issue guidelines- Rule 9(14)

(vii) Reporting entities to formulate and implement CDD program- Rule 9(14)(ii)

h) Sunset clause for closing of accounts which are not KYC compliant – Rule 10(3)

i) Time limit for furnishing report to Director u/s 13(2)(c)- Rule 10 A

j) Expenses for audit -10 B

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 Act was amended from 1st February, 2013 to make it more effective in preventing unlawful activities and meet the standards of the Financial Action Task Force. The salient features of the amendment 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 enlarging the ambit of 'terrorist act' by incorporating production or smuggling or circulation of high quality counterfeit Indian paper currency, coin or of any other material. 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 listed in Second Schedule to this Act;

(3) Raising funds for terrorist act to include raising of funds, both from legitimate or illegitimate sources, by a terrorist organization or by terrorist gang or by an individual terrorist;

(6) Offences by companies, societies or trusts brought in the ambit of the Act and punishments therefor provided for;

(7) Enlargement of the scope of proceeds of terrorism to include any property intended to be used for terrorism; and

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

(i) attachment or forfeiture of property equivalent to the counterfeit Indian currency involved in the offence;

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

(iii) confiscation of movable or immovable property on the basis of the material evidence where the trial cannot be concluded for various reasons.

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 companies, financial institutions and designated non-financial businesses and professions to maintain records of all transactions, furnish information of prescribed transactions to Director, FIU-IND and to verify the identity of their clients and their beneficial owners in the manner prescribed. The reporting entities are also required to preserve records of transactions and records of identity of clients for a period of five years. The PML (Maintenance of Records) Rules prescribe the requirements for maintenance of records and reports to be submitted to FIU-IND. The obligations of the reporting entities are summarized at Appendix E. Section 12A empowers the Director to call for additional information from reporting entity apart from records referred to in 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 14 of the PMLA provides that the reporting entity, its Directors and employees shall not be liable to any civil or criminal proceedings against them for furnishing information to FIU-IND. Section 50 bestows upon Director, FIU-IND powers vested in a civil Court under the Code of Civil Procedure, including powers to enforce attendance of any person, compel production of records, receive evidence on affidavits and issuing commission for examination of witnesses. Section 54 empowers and requires various officers and other functionaries to provide necessary assistance to Director, FIU-IND in the enforcement of his statutory functions under the PMLA.

Section 66 provides for the dissemination of information by FIU-IND to any officer, authority or body performing any function under any law relating to imposition of any tax, duty or cess or to dealing in foreign exchange or to prevention of illegal trafficking in drugs or to any officer, authority or body notified by the Central Government.

Section 69 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

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

Financial Institutions

- Insurance companies
- Hire purchase companies
- Chit fund companies
- Housing finance institutions
- Non-banking financial companies
- Payment system operators*
- Authorized persons
- India Post

Intermediaries

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

DNFBP

- Casino
- Registrar 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.)

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. These reports are analysed and results of analysis are disseminated to the 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 have 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 furnish all their reports to FIU-IND online using its FINgate portal. The FinCore portal of the FINnet processes the report received from the reporting entity and links all relevant reports available in the database using rules of identity and relationship resolution. A case formed around a suspicious transaction report thus contains not only the information received from a particular reporting entity but also all relevant information/ reports 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.

The number of STRs received, analysed and disseminated has shown increasing trend. Focused 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 (CTRs)

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 individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of rupees ten lakh or its equivalent in foreign currency.

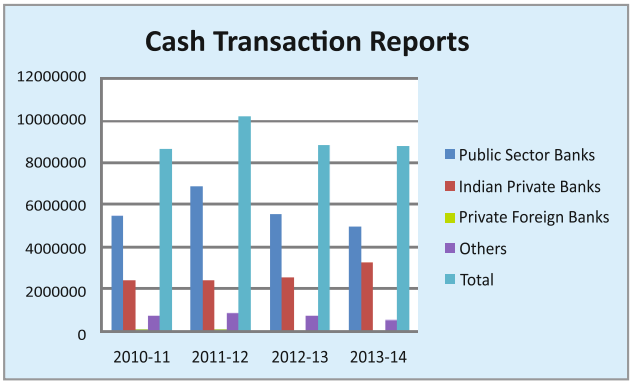
Cash Transaction Reports for the month are to be furnished by the 15th day of the succeeding month.

Majority of the CTRs received during the year continued to be from the Public Sector Banks, which have the largest number of bank accounts and the largest share of deposits held by them. Consistent efforts were made

to ensure that the smaller banks such as district co-operative banks and regional rural banks do not face difficulty in adopting the new technology for filing of CTRs and other reports online. However 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 after the FINnet became operational. FIU-IND is making all out efforts to train the key persons in the banks for filing of reports online. The reporting entities are also being 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 -2):

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

Types of Banking companies	2010-11	2011-12	2012-13	2013-14
Public Sector Banks	54,63,252	69,03,096	55,41,408	49,89,143
Indian Private Banks	24,42,286	24,06,855	25,61,548	32,61,219
Private Foreign Banks	1,05,288	83,665	58,640	35,083
Others	6,76,281	8,04,646	7,20,622	4,93,637
Total	**86,87,107**	**1,01,98,262**	**88,82,218**	**87,79,082**



Suspicious Transaction Reports (STRs)

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-clauses (b) and (c) of the definition of suspicious transaction given above.

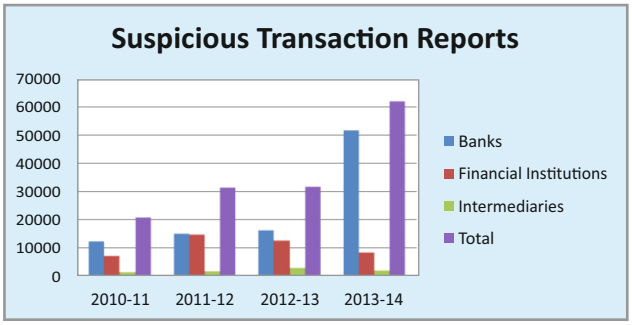
Suspicious Transaction Reports (STRs) are required to be furnished by the principal officer of the reporting entity not later than seven working days on being satisfied that the transaction is suspicious.

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, Card System Operators, insurance sector and capital market sector.

The "Train the Trainers" programme conducted once a year by FIU-IND has produced the desired chain effect in spreading AML/CFT awareness across the reporting entities. The resource persons 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.

Table 3:Receipt of Suspicious Transaction Reports:

Reporting Entity Type	2010-11	2011-12	2012-13	2013-14
Banks	12,287	14,949	16,284	51,765
Financial Institutions	7,006	14,712	12,637	8,321
Intermediaries	1,405	1,656	2,810	1,867
Total	20,698	31,317	31,731	61,953



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

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

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

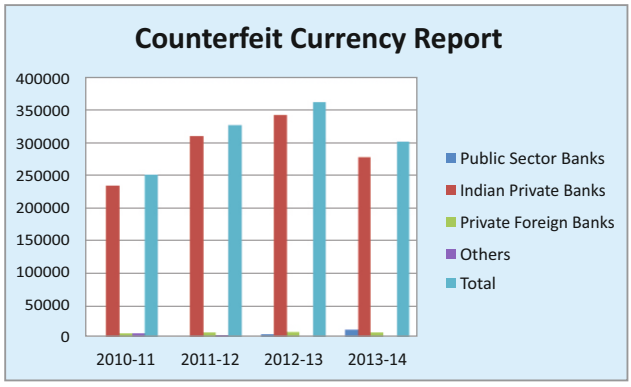
In terms of the business risk categories, the document draws on the FATF's risk-based approach guidance document; and, in terms of the alert indicators, it differentiates between those that are relevant at the branch level and those that apply at the level of the centralised AML monitoring unit. The report identified 88 red flag indicators relating to 10 sources of alert.

Counterfeit Currency Reports

PMLA and PML Rules require reporting entities 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.'

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

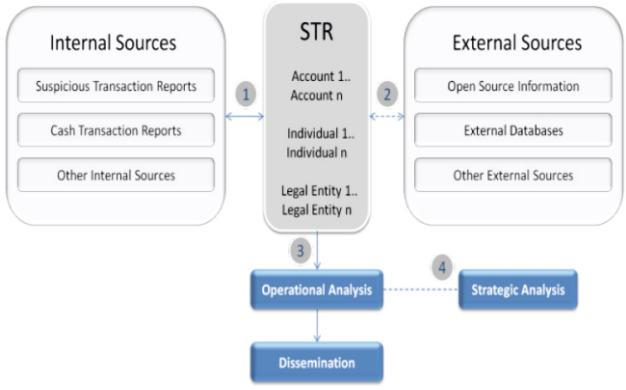
Reporting Entity Types	2010-11	2011-12	2012-13	2013-14
Public Sector Banks	1,896	2,649	5,707	14,186
Indian Private Banks	2,34,400	3,10,714	3,43,358	2,78,240
Private Foreign Banks	7,936	9,273	10,489	8,331
Others	7,216	4,746	2,817	1,047
Total	2,51,448	3,27,382	3,62,371	3,01,804



During the year, CCR reporting continued to remain a thrust area. The private Indian Banks contributed majority of CCRs (Table-4). The compliance levels of the public sector banks continued to be low despite the matter having been taken up with the RBI to take necessary steps for improvement. 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 offences and terrorist financing and to disseminate the results 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 and distinguished between operational and strategic analysis. The process of analysis of STRs is depicted below:



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

should be disseminated and to which agency:

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

Table 5: Analysis of Suspicious Transaction Reports

Category	2010-11	2011-12	2012-13	2013-14
STRs received	20,698	31,317	31,729	61,953
STRs brought forward from previous year	1,118	1,775	1,813	14,876
STRs Processed	20,041	31,279	18,666	35,696
STRs Disseminated	13,744	23,689	13,854	15,288

Dissemination

FIU-IND disseminates STRs which are considered relevant for investigation by law enforcement/ intelligence agencies based on the nature of suspicion, predicate offence involved and other relevant information linked with the STR. With the launch of the 'FINnet' in October 2012, the STRs are processed using the 'FINcore' module of the solution. 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 for feedback for each case disseminated.

Table 6: Dissemination of Suspicious Transaction Reports

Agencies	2010-11	2011-12	2012-13	2013-14
Law Enforcement Agencies	8,826	16,905	12,497	13,931
Intelligence Agencies	5,523	10,905	3,730	3,146
Regulators & others	127	225	192	452
Total	**14,476**	**28,035**	**16,419**	**17,529**

Note: One STR can be disseminated to more than one agency

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 (RBI, SEBI, IRDA) and foreign FIUs. Statistical information relating to dissemination of intelligence reports during the year 2013-14 is given in Table-6. Some STRs are disseminated to more than one agency and hence, the number of dissemination reports is higher than the number of STRs disseminated.

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. One of the companies registered in Singapore was 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. Total payout promised to these subscribers was approximately INR 300 billion (USD 5 billion approx.).

A number of banks filed STRs in respect of the entities and individuals involved in this fraud. FIU-IND could link 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 abroad, which were disseminated to various LEAs.

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 was being further investigated. Tax authorities froze three bank accounts containing a sum of USD 22 million and levied substantial tax, interest and penalty against one of the Singapore based companies and two of its master distributors in India.

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. Moreover, 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
  - o LEAs/IAs
  - o Foreign FIU
- CTR Analysis Reports – Cluster of CTRs related to
  - o High Risk Businesses
  - o High Risk Geographic Locations
  - o 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

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

A. Preventing misuse of the financial system

Financial institutions (reporting entities) are often the front-line 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 financial 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 PMLA Rules was amended in May 2007 to specifically provide for reporting of suspect transactions relating to terrorist financing. The success of AML/CFT regime is critically dependent on the capability of the reporting entities in identifying and reporting suspicious transactions. FIU-IND has been actively involved in sensitizing reporting entities about their obligation to report STRs related to suspected cases of terrorist financing and providing guidance on detection and reporting of such transactions.

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

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

Table 7 – Requests received from Intelligence Agencies

Category	2010-11	2011-12	2012-13	2013-14
Requests received from Indian intelligence agencies	428	473	457	373

D. Information exchange with foreign FIUs on terrorism financing cases

FIU-IND was admitted as a member of the Egmont Group of FIUs in May, 2007. FIU-IND is regularly sharing information with foreign FIUs over Egmont Secure Web on suspected money laundering and terrorist financing cases. FIU-IND has signed MOUs with 24 countries including 5 MoUs signed in 2013-14. FIU-IND, however, does not decline a request for information due to absence of MoU.

E. Contribution to global efforts to combat financing of terrorism

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

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

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

Chapter 4

Domestic and International Cooperation - Building Partnerships

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

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

Several workshops were held to explain to the users of domestic agencies the framework of this information exchange. Demonstration of the functionality of the bulk request utility to generate XML and input XML was also given using sample data.

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 comprises 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) 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 STR. The template is being used by the members for reporting feedback to FIU-IND. The Virtual Office has proved to be an effective forum for exchange of information among the tax agencies.

Feedback received through the Virtual Office platform reveal that based on the STRs disseminated by FIU-IND, CBDT authorities have been able to detect unaccounted income of Rs.7,078 crore and to make a seizure of unaccounted assets valued at Rs.163 crore. Similarly, the CBEC authorities have detected evasion of service tax and excise duty amounting to over Rs.750 crore and seized assets worth Rs.17 crore. The STRs of FIU-IND have also been instrumental in detection of proceeds of crime of about Rs.20 crore and seizure/ attachment of assets worth about Rs.15 crore by the Enforcement Directorate. STRs disseminated by FIU-IND have also formed the basis for institution of 105 new Economic Crime Information Reports (ECIRs) by the Enforcement Directorate.

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 designated a dedicated nodal officer to deal with all issues relating to these 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 rely on information contained in FIU-IND databases not only for developing intelligence but also for strengthening ongoing investigations. During the year, FIU-IND provided information to various agencies in response to 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	2010-11	2011-12	2012-13	2013-14
Requests received from Intelligence Agencies	428	473	457	373
Requests received from Law Enforcement Agencies	186	117	92	221

Memorandum of Understanding (MOUs)

FIU-IND has entered into Memorandums of Understanding (MoUs) with partner agencies in order to provide a structural framework for enhanced cooperation and understanding. The MOU provides for protection of the information disseminated by FIU-IND from unauthorized use and proliferation and for application of confidentiality and data protection benchmarks throughout the chain of transmission of information in the agencies receiving the information. In pursuance of these objectives, MoUs have been signed with RBI, MCA, SFIO, CBI, NCB, CBDT, CBEC, NIA, IRDA and SEBI.

Signing of MoU with Central Board of Direct Taxes (CBDT)

Signing of MoU with National Investigation Agency (NIA)

Signing of MoU with Central Board of Excise & Customs (CBEC)

Signing of MOU with Insurance Regulatory and Development Authority (IRDA)

Signing of MOU with Central Bureau of Investigation (CBI)

Signing of MOU with Narcotics Control Bureau (NCB)

Regulators

FIU-IND has also developed close relationship with financial system regulators for strengthening AML and CFT regulations. These 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), Pension Fund Regulatory & Development Authority (PFRDA) and Forward Market Commission (FMC) have issued instructions/ guidelines to the financial sector entities for adherence to KYC, AML and CFT norms. FIU-IND has ensured that suitable modifications are carried out in their Circulars, wherever necessary. These Circulars are also uploaded on the website of FIU-IND for quick reference.

FIU-IND continued its regular interaction with the Regulators, industry associations and self-regulatory organisations (SROs) 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 the 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 the year, 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 provided 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 visited 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. 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.

FIU-IND is also represented in the India-Russia-USA Trilateral Working Group on Financial aspects of Afghan Drug Trade, where it is regularly exchanging information with other trilateral partners on drug related offences.

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-F.

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 2013 at Oslo, Norway and in October 2013 at Paris, France.

FIU-IND has provided important suggestions and inputs 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 issued by the FATF in 2013.

National ML/ TF Risk Assessment

In 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. During 2013-14, the AML-SC constituted Sector-specific Working Groups (SWGs) for the banking, insurance and capital market sectors under the chairmanship of the Regulator concerned. These SWGs have members drawn from LEAs, Regulators, FIU and industry associations and their mandate is to carry out the risk assessment of their sector.

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.

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)

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 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.

The 17th Annual Meeting of APG was held at Shanghai, China, which was attended by the Director. FIU-IND has also provided an expert in the Mutual Evaluation Working Group (MEWG) of the APG to oversee various mutual evaluations conducted by APG of its member countries.

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.

Follow-up Process and Recommended Action for FIU-IND

India was admitted as a Member of the FATF in June 2010 and 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). FIU-IND took systematic and concrete steps in the areas of deficiency to become compliant with the FATF standards.

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.

In response to the comments in the MER, 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 34 training programmes involving over 2,400 participants, and have also run a Train-the-Trainer course for 160 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.

The progress made by India to remove the deficiencies pointed out in the Mutual Evaluation has been periodically reviewed by the FATF. In the “8th Follow-Up Report of India's Mutual Evaluation” published by the FATF in June 2013, it has been commented that with respect to the suspicious transactions reporting regime, the FIU has further

enhanced its outreach programme to provide guidance to the financial sector on their reporting obligations, and has engaged in extensive compliance monitoring. The result has been a significant increase in the number of STRs filed both with respect to ML and TF, without any evidence that this constitutes defensive reporting.

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 over 140. Member FIUs 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 protection of confidentiality. The information exchanged under Egmont Principles is used for intelligence purposes only and cannot be used for any other purpose without prior consent of the providing FIU.

FIU-IND was admitted as a member of the Egmont Group at the Bermuda Plenary session in May 2007. During the month of June 2007, Egmont Secure Web (ESW) was also made operational for exchange of information over a secure network.

Officers of FIU-IND have regularly participated in the Egmont Group meetings. During the year, FIU-IND participated in the 21st Annual Plenary session of Egmont Group at Sun City, South Africa in July 2013 and the Egmont Committee and Working Group Meetings at Budapest, Hungary in February 2014. 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.

FIU-IND continued to be the one of the two regional representatives of the Asia region, 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. FIU-IND actively participated in the CRP by regularly to various issues identified by CRP for detailed examination. This gave 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 contributed detailed papers on the issues assigned to FIU-IND and also provided substantive comments on issues dealt with by other FIUs.

Director, FIU-IND (right most) attending the Asia region meeting of Egmont Group at Sun City, South Africa in July 2013 (Photo courtesy: qfiu.gov.qa)

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 9.

Table 9: Exchange of information with foreign FIUs

Status of action Taken	2010-11	2011-12	2012-13	2013-14
Requests received from foreign FIUs	93	113	97	94
Requests sent to foreign FIUs	67	46	81	82
Spontaneous referrals received from foreign FIUs	14	22	26	51
Spontaneous referrals made to foreign FIUs	6	24	11	0

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. During 2013-14, MOUs were signed with the FIUs of Thailand, Guernsey, Montenegro, South Africa and Ukraine. MoUs with more than 15 countries are under various stages of negotiation.

Signing of MoU with FIU of Ukraine on the margins of Egmont Group meeting at Budapest, Hungary, February, 2014.

Signing of MoU with APML Montenegro at Sun City, South Africa, July 2013.

Signing of MoU with FIC South Africa at Sun City, South Africa, July 2013.

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 participated in the meetings of Working Groups with various countries. FIU-IND participated in the meetings of Joint Working Groups with Thailand and the USA, for example.

Chapter 5

Raising awareness and building capacities of reporting entities

Banking companies, financial institutions (insurance companies, housing finance companies, non-banking finance companies, chit fund companies, payment system operator, authorised money changers and casino), intermediaries of securities market and DNFBPs, collectively referred to as "reporting entities" have reporting obligations under the PMLA. 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 capacities to ensure better compliance.

A significant step taken in enabling the reporting entities to efficiently identify suspicious transactions was to prescribe a 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 prescribed 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 by Regulators and the 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 34 workshops/interactions on AML/CFT awareness in collaboration with regulators, industry associations, professional bodies and reporting entities, targeted at over 2,400 participants. The statistics relating to training seminars and workshops are in Table 10.

During the year, FIU-IND focused on training the reporting entities in various sectors on online filing of reports on the FINnet portal. FIU-IND also focused on enhancing awareness of cooperative banks and Regional Rural Banks (RRBs) about their reporting obligations under the PMLA.

Twenty five review meetings were conducted with the Principal Officers of the reporting entities in various sectors covering 580 officers. A number of meetings were also held with the Designated Directors of the banks and financial institutions so as to create AML/CFT awareness at the top management level.

Outreach Activity	2010-11	2011-12	2012-13	2013-14
Seminars and Training workshops	50	42	38	34
Number of Participants	2,264	2,509	2,862	2,447
Review Meetings	31	39	28	25
Number of Participants	435	977	1,471	580

'Train the Trainers Programme'

FIU-IND organized a two-day “Train the Trainers” workshop on AML/CFT at National Stock Exchange (NSE) Building on 13-14 March, 2014. This was the seventh consecutive annual workshop organized by FIU-IND for the trainers in the financial sector. 160 senior officers of the public and private sector banks, insurance companies, Government Departments and faculty members of staff training colleges and institutes of banks 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 such as the recent amendments to PMLA, revised FATF guidelines, risk-based approach for effective detection of suspicious transactions and technical issues relating to filing of statutory reports.

Director, FIU-IND addressing the participants of “Train the Trainer” Workshop, March 2014 at NSE, Mumbai

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 and Designated Directors of the reporting entities to provide guidance and feedback on their reports. Some meetings were in the nature of compliance reviews, where AML/KYC policies and procedures were reviewed and lapses 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 11). 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 11 - Review Meetings with Principal Officers

Month	Review meeting held with
April,2013	Private Banks
May,2013	Urban Cooperative Banks
	MTSS
June,2013	Credit Cards Operators
	MTSS
July,2013	Money Transfer Agents
	Coop. Bank
August,2013	Money Transfer Agents
September,2013	Law Enforcement Agencies
	Money Transfer Agents
	Regulators
	Money Transfer Agents
	Mutual Funds
	Public Sector Banks & FPFBs
October,2013	Public Sector Banks & FPFBs
	Insurance Regulatory and Development Authority (IRDA)
	Pension Funds Regulatory and Development Authority (PFRDA)
	Life Insurance Companies
	Non-Life Insurance Companies
November,2013	Public Sector Banks
	Payment System Operators
December,2013	Public Sector Banks
	FIU-IND
January,2014	IRDA
	RBI

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. 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 with 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 Vertical headed by an Additional Director to act as nodal point for enforcing compliance and for corrective action in cases of non-compliance. This Vertical 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 all the three principal Regulators i.e. RBI, SEBI and IRDA. This has enabled a regular and structured exchange of information between RBI and FIU-INDIA, resulting in better compliance monitoring.

During the year, 594 advisories were issued to reporting entities highlighting problem areas and advising them to improve their compliance under PMLA. In 2 cases fines were imposed by FIU-IND under section 13 of the PMLA.

The details of advisories issued are as under:

Table 12- Sector-Wise Statistics of Advisories issued

S.No.	Category	No. of Advisory issued till 31. 03.14
1	Casinos	17
2	Public Sector Bank	21
3	Intermediary	122
4	MTSS Cards	5
5	Private Banks	14
6	Insurance	13
7	Co-Operative Banks	179
8	Others	223
		594

Chapter 7

Organizational Capacity Building

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

With a view to enhance the capacity of its officers and to impart to them the knowledge of various sectors of the financial system in India, FIU-IND continues to collaborate with premier training institutes for targeted training relating to various financial sectors, financial instruments, sector-specific laws and regulations, financial crimes, regulatory framework, 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 13) including insurance frauds, data analytics, intelligence tradecraft, capital market frauds, cyber-crimes, etc.

Table 13: Capacity Building Workshops attended by Officers from FIU-IND

MONTH	WORKSHOP	ORGANISED BY	PLACE
May 2013	Training programme on "Prevention of Insurance Frauds"	National Insurance Academy	Pune
Jun 2013	Training of "IDFA Boot Camp"	Sama Audit Sys & Software Pvt Ltd	Mumbai
Jun 2013	Training of "IDFA Boot Camp"	Sama Audit Sys & Software Pvt Ltd	Mumbai
Jun 2013	Training of "IDFA Boot Camp"	Sama Audit Sys & Software Pvt Ltd	Mumbai
Jun 2013	Training of "IDFA Boot Camp"	Sama Audit Sys & Software Pvt Ltd	Mumbai
July 2013	Training programme on "Banking Laws & Fiscal Laws Enforcement"	State Bank Staff College	Hyderabad
Sep 2013	Training programme on "Intelligence Gathering & Intelligence Tradecraft"	Military Intelligence Training School & Depot	Pune
Oct 2013	Training programme on "Investigating Economic Crimes in Financial Markets"	IICM, Mumbai	Mumbai
Oct 2013	Training programme on "Investigating Economic Crimes in Financial Markets"	IICM, Mumbai	Mumbai
Oct 2013	Training programme on "Investigating Economic Crimes in Financial Markets"	IICM, Mumbai	Mumbai
Dec 2013	Training programme on "Intelligence Gathering & Intelligence Tradecraft"	IB Central Training School	New Delhi
Feb 2014	Course "Investigation of Internet Based Crime & Open Source Intelligence"	SVP National Police Academy	Hyderabad

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 Feb 2010. FINnet Gateway report upload module went live on 20th October 2012 and the reporting entities began uploading of reports in the XML reporting format on the Gateway. The complete solution was accepted on 22nd March 2012.The SI would provide enhanced support for 1 year from the date of 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.

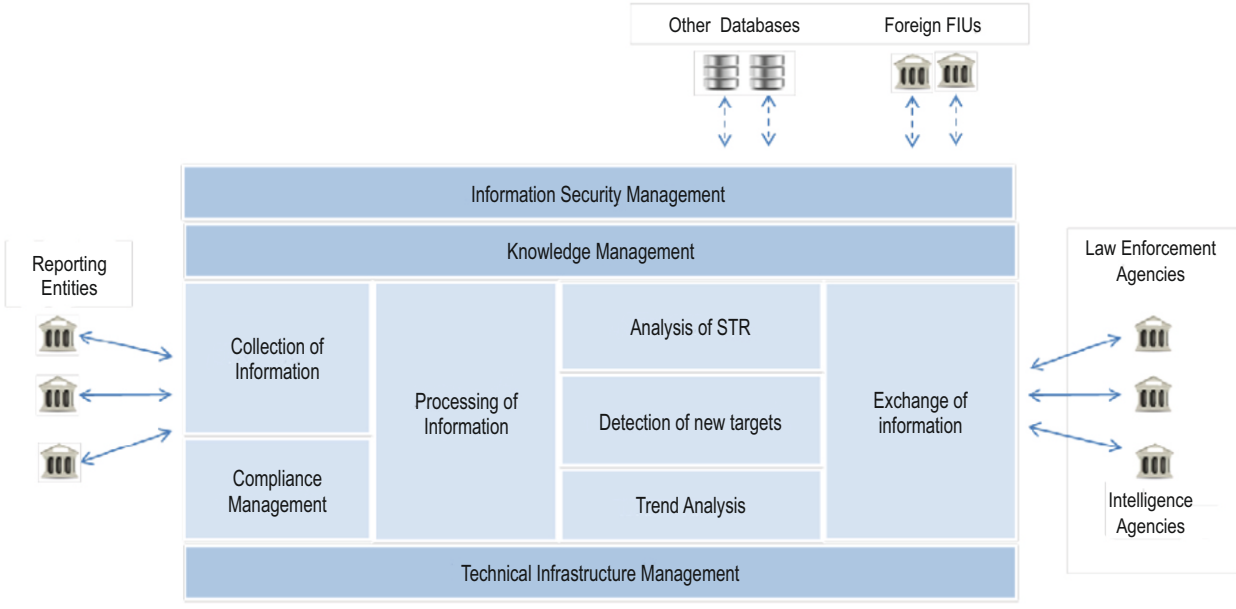


Figure: Schematic overview of FINnet

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.

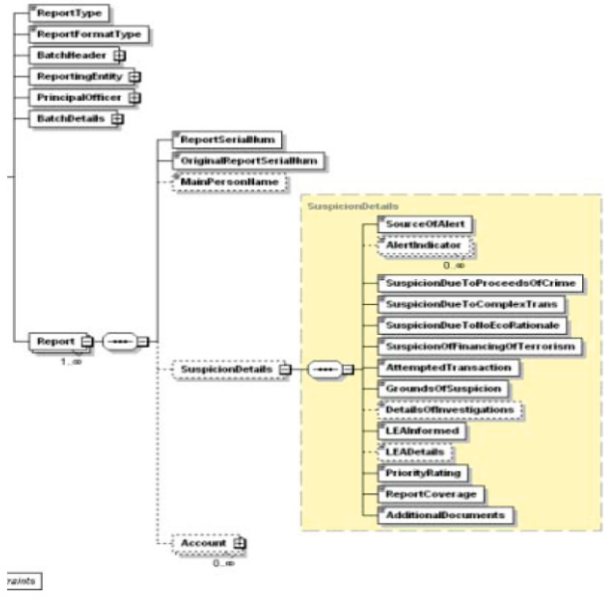


Figure: XML format specification of report

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

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

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

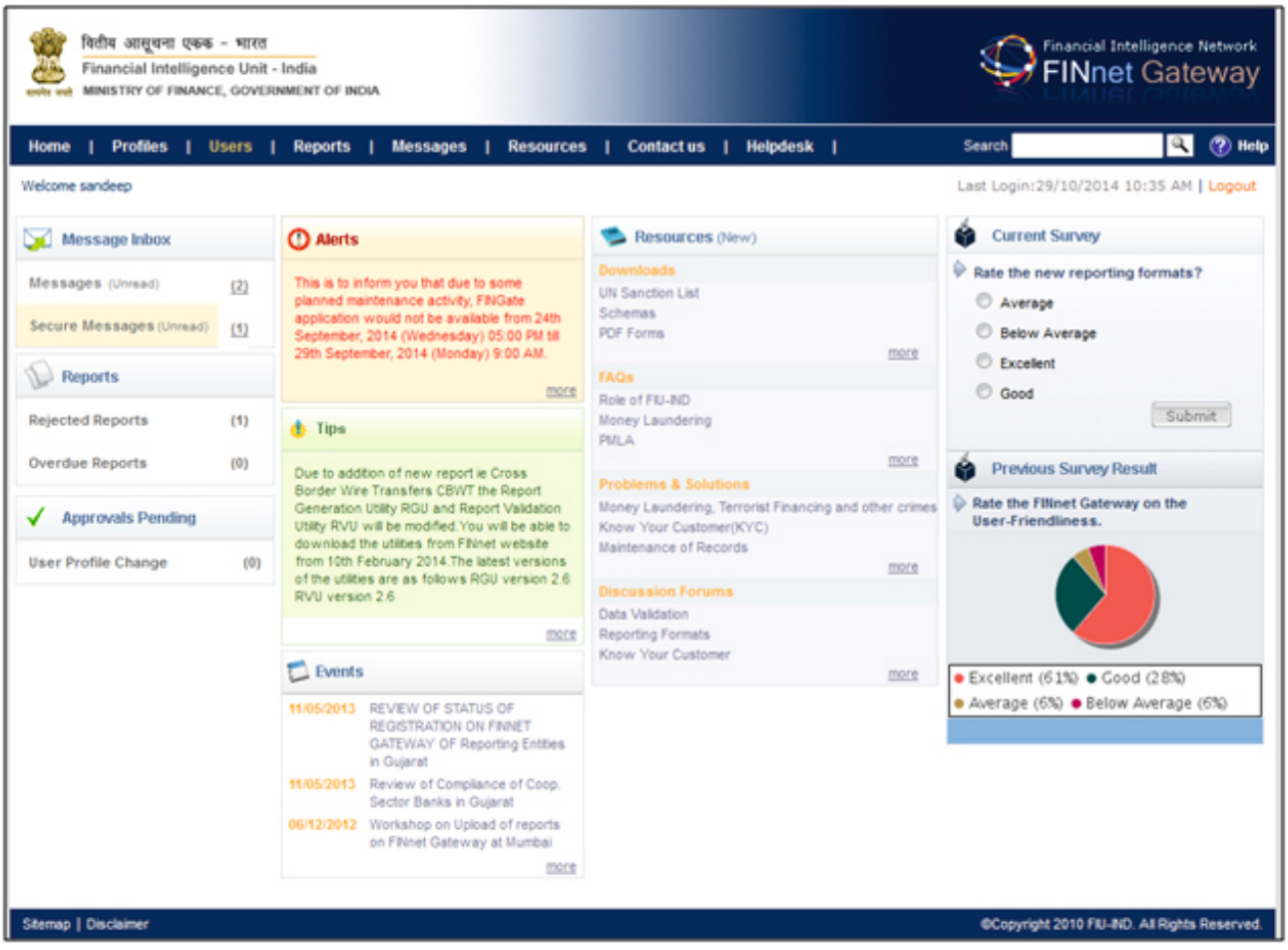


Figure: FINnet Gateway Portal for reporting entities

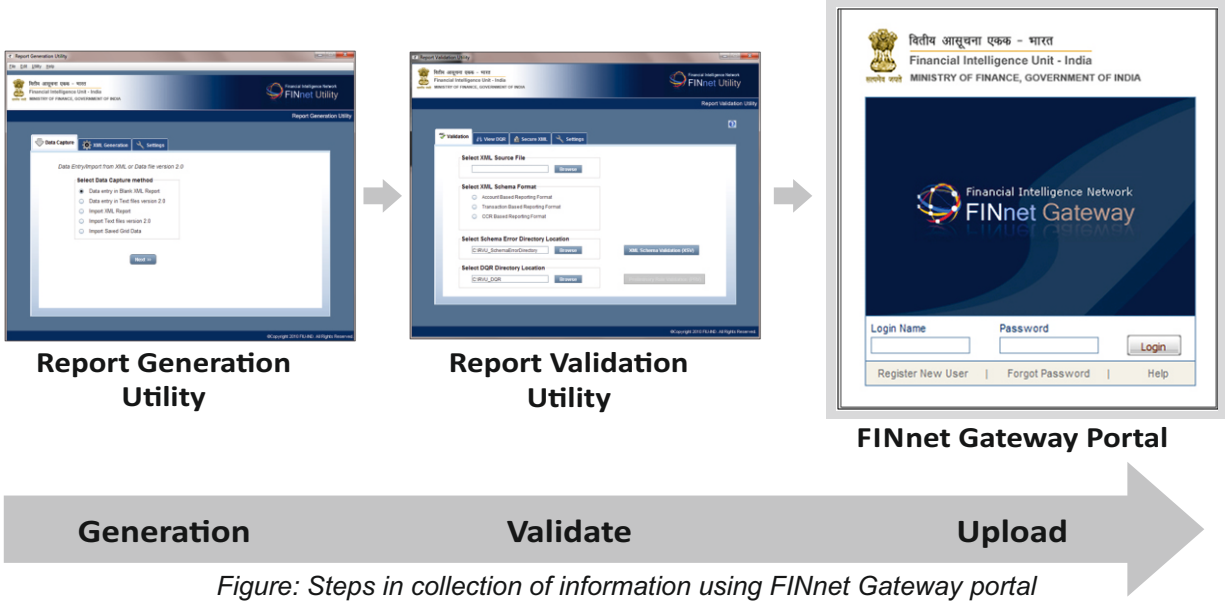


Figure: Steps in collection of information using FINnet Gateway portal

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.

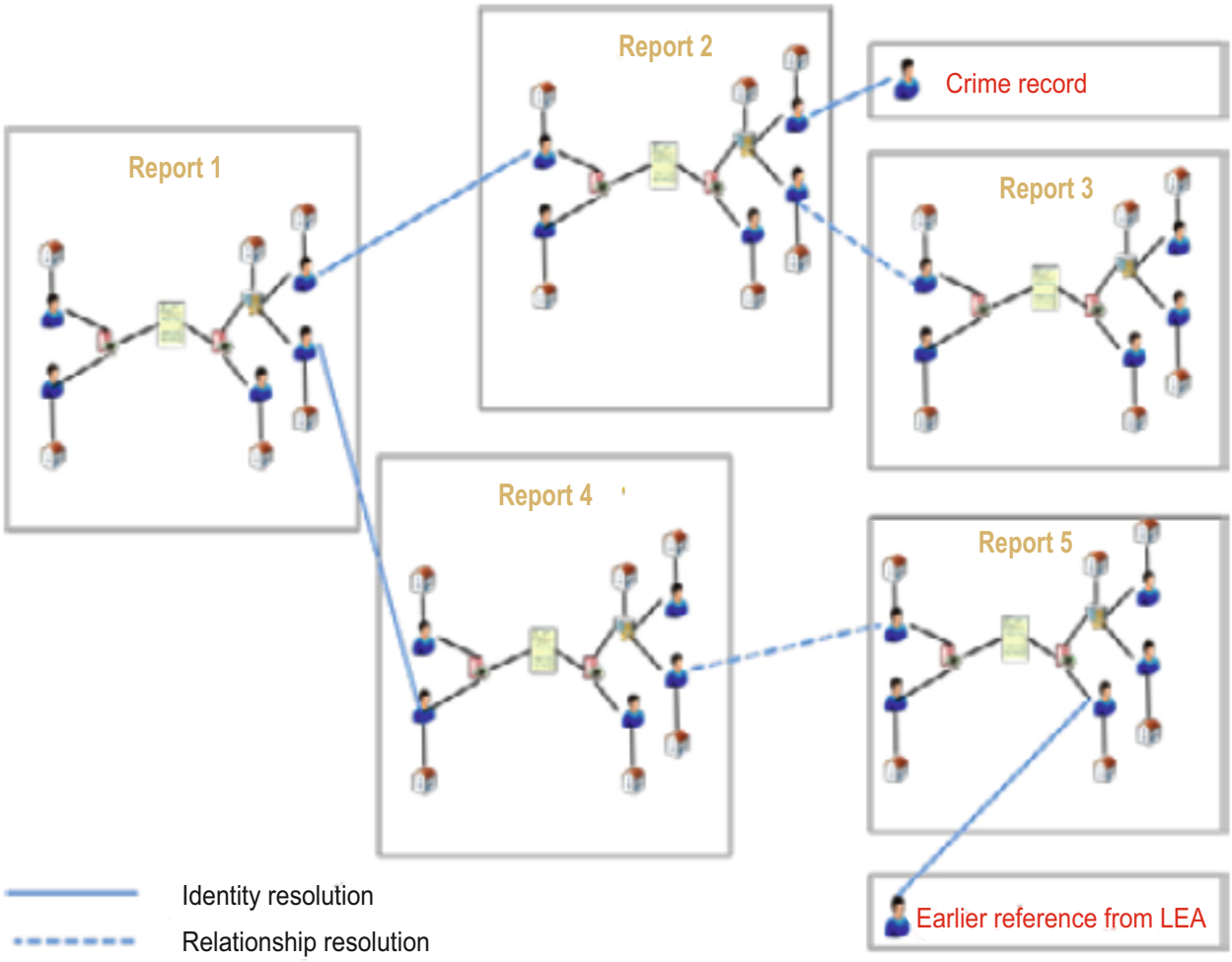


Figure: Clustering of report by Identity and Relationship Resolution.

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.

Operational Analysis of Reports (CTR, STR, NTR)

Operational Analysis of Cash Transaction Reports (CTR) is based on Alert Management System which utilizes the risk based approach. A comprehensive risk management system consisting of data mining tools 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 with FIU-IND and second is identification of new target by generating a list view.

Strategic Analysis

Strategic Analysis of database is built around the 'Trend Module' of FINcore. It uses business intelligence software to identify trends in reports, suspicion types, counterfeit currency incidents, remittances and card transactions. The trends can be analyzed 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.

Compliance Management

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

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

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. FIU-IND also initiated the process of obtaining ISO 27001:2013 Certification of its I.T. systems and aims to get the Certificate by the end of 2014-15.

Future Challenges

FINnet has substantially enhanced the efficiency and effectiveness of FIU-IND's core function of collection, analysis and dissemination of financial information. IT enablement of key processes ensures higher productivity, faster turnaround time and effective monitoring in all areas of FIU-IND's work. The current focus is to internalize the new reports introduced in PMLA amendments of 2013 i.e. Cross Border Wire Transfer Report and reports from Registrars and Sub-registrars of property. System up-gradation is also required to cater to the large volumes of reports being filed.

Appendix-A : Staff strength of FIU-IND

Post	Sanctioned Strength	Working as on March 31, 2014
Director	1	1
Additional Director / Joint Director	10	10
Technical Director	1	1
Joint Director Systems (earlier Principal System Analyst)	1	0
Deputy Director Systems	2	0
Deputy / Assistant Directors (earlier Senior Technical Officer)	21	13
Assistant Director Systems (earlier System Analyst/Programmer)	6	0
Group B, C & D	33	7
Total	75	32*

** In addition 31 persons were working on contract basis.*

FIU-IND Team: List of Officers

Praveen Kumar Tiwari	-	Director
Amitav	-	Additional Director
Anand Jha	-	Additional Director
Ms. Renu Amitabh	-	Additional Director
Rajendra Singh	-	Additional Director
Sanjay Bansal	-	Additional Director
Ms. Deepika Mittal	-	Additional Director
Satyendra Narayan Pandey	-	Additional Director
Chaitanya Shukla	-	Joint Director
Ashok Kumar	-	Joint Director
Sanjay Kumar	-	Joint Director
D. Rajasekar	-	Technical Director (NIC)
Naresh K. Bhatia	-	Deputy Director
Anand Y. Gokhale	-	Deputy Director
K.K. Verma	-	Deputy Director
Sanjay Kumar Sharma	-	Deputy Director
Pramod Kumar	-	Deputy Director
A. Ramesh	-	Deputy Director
S.D. Sharma	-	Deputy Director
Ajay Sachdev	-	Deputy Director
Vijay Saxena	-	Deputy Director
Dinesh Kumar	-	Deputy Director
Ajay Sharma	-	Deputy Director
Tassine Sultan	-	Assistant Director
Ms. Seema Chakrabarty	-	Assistant Director
Ms. Pawanjeet Kaur Rishi	-	Consultant
Warren Francis	-	Consultant

Mr. Tassine Sultan, Assistant Director, FIU-IND has been granted Presidential Award for 'Specially Distinguished Record of Service' on the occasion of Republic Day, 2014.

Appendix-B : Chronology of Events for 2013-14

May 20-24, 2013	EAG plenary and Working Group Meetings at Belarus
June 17-21, 2013	FATF Working Gp & Plenary Meetings at Norway
June 30 - July 05, 2013	21st Egmont Plenary Meetings at South Africa
July 15-19, 2013	APG's 16th Annual Meeting and technical assistance forum meeting at China
Sept. 10-11, 2013	Australian sponsored workshop on the threats and vulnerabilities of money laundering in the capital markets in South Asia at Colombo
Sept. 23-25, 2013	Asia Pacific Economic Cooperation (APEC) Pathfinder Conference at Bangkok
Oct. 13-14, 2013	Egmont Committee Inter-sessional Meeting at Paris
Nov. 25-27, 2013	Training program on “AUSTRAC's approach for collection, analysis, dissemination of their International Fund Transfer Report” at Australia
Dec. 03-04, 2013	Meeting - AML & Compliance Asia 2013 at Singapore
Dec. 02-06, 2013	A team visited Royal Monetary Authority of Bhutan to provide technical assistance for developing FIU
Dec. 03-04, 2013	"India-Russia-USA Trilateral Working Group on Financial aspects of Afghan Drug Trade" Meeting at Moscow
Feb. 16-19, 2014	Egmont Committee and Working Group Meetings in Hungary
Feb. 27-28, 2014	5th Meeting of India - Uzbekistan JWG-CT at Tashkent
Mar. 29-31, 2014	FIU Regional Cooperation Seminar at Abu Dhabi, organized by Central Bank of UAE

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 (PMLA) shall come into force.
01.07.2005	2/2005	Appointed an Adjudicating Authority to exercise jurisdiction, powers and authority conferred by or under the PMLA. 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 PMLA 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 PMLA.
01.07.2005	5/2005	Conferred certain exclusive and concurrent powers under the PMLA to the Director, Financial Intelligence Unit, India.
01.07.2005	6/2005	Conferred certain exclusive and concurrent powers under the PMLA 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 PMLA.
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 PML 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 : 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 he 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 Cross Border Wire 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-F: 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).
- Re banducing 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.d out through an account in the customer's name with ak subject to similar CDD standards.

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

Recommendation 11 (Record-keeping)

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

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

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

Recommendation 12 (Politically exposed persons)

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

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

b. obtain senior management approval for establishing (or continuing, for existing

customers) such business relationships;

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

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

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

Interpretive Note

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

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

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

Recommendation 15 (New technologies)

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

Recommendation 16 (Wire transfers)

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

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

Recommendation 17 (Reliance on third parties)

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

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

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

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

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

Recommendation 18 (Internal controls and foreign branches and subsidiaries)

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

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

Interpretive Note

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

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

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

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

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

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

Recommendation 20
(Reporting of suspicious transactions)

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

Interpretive Note

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

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

Recommendation 21
(Tipping-off and confidentiality)

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

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

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

Recommendation 22 and 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 Vfinancial institutions and DNFBPs)

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommend-ations. 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.

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	entral 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
IA	Intelligence Agency
IB	Intelligence Bureau
IBA	Indian Banks' Association
ICAI	Institute of Chartered Accountants of India
IMF	International Monetary Fund
IRDA	Insurance Regulatory and Development Authority
ISPP	Information Security Policies and Procedures
JWG	Joint Working Group
KMS	Knowledge Management System
KYC	Know Your Customer
LEA	Law Enforcement Agency
MEQ	Mutual Evaluation Questionnaire
MER	Mutual Evaluation Report
MHA	Ministry of Home Affairs
MoU	Memorandum of Understanding
NABARD	National Bank for Agriculture and Rural Development
NBFC	Non-banking Financial Company
NCB	Narcotics Control Bureau
NHB	National Housing Bank
NSCS	National Security Council Secretariat
NTR	Non- Profit Organisation Transaction Report
OpWG	Operational Working Group (of the Egmont Group)
PDC	Primary Data Centre
PFRDA	Pension Funds Regulatory and Development Authority
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

Visit by officers from FIU of Bangladesh and Anti-Corruption Commission (ACC), Bhutan to FIU-IND in May, 2013

Visit by delegation from Ethiopian Government to FIU-IND in March, 2014

Participants and FIU-IND officers at 'Train the Trainer Programme' at NSE, Mumbai, March, 2014

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)**