

Money Laundering & Terrorist Financing Risks
Quick Summary by Pramod Khandelwal

Index

Sr	Particulars	Page No
I	Money Laundering and Terrorist Financing Risks	2
II	International Norms	3
III	AML/ CFT Framework in India	4
IV	Organizational Set-up in Bank/ FI	5
V	Legal & Regulatory Provisions – Salient Features	6
VI	Customer Due Diligence	6
VII	Customer Risk Categorization	7
VIII	FIU – Reporting	7

I. Money Laundering and Terrorist Financing Risks

A. Concepts of Money Laundering and Terrorist Financing

Banking and finance sector activities carry several risks which depend on the nature of products and services. There are three risks that are inherent to all financial activities, viz. Money Laundering, Terrorist Financing, and Financial Crime. These risks are distinct but are closely interconnected too.

Money Laundering: It is the process of disguising the source of money raised through criminal activities i.e. illegal money and induct it with a view to make it appear to emanate from legal activities i.e. legal money and deploy it in legal avenues. The process of money laundering is a criminal offence in itself, besides the predicate criminal offence, the source of illegal funds.

Terrorist Financing: Terrorist financing includes providing financial resources or material support for the purpose of carrying out terrorist activities, or running terrorist outfits, or for other activities carried out by terrorist outfits or other organisations supporting these outfits. Terrorist financing of course is criminal offence.

Financial Crimes: These cover host of activities that involve illicit financial gains to the perpetrators by defrauding general public (like collecting funds from public with intention to defraud them), tax related frauds, tax evasion, corruption, bribery, etc. All such activities are criminal offences under various laws.

Persons engaged in these crimes are heavily dependent on banks and other financial institutions for various financial transactions for the purpose of moving and storing them till these are ultimately used for their desired purpose. By definition, whenever a financial crime occurs through financial system money laundering coexists. It is also found that money laundering is also resorted to for terrorist financing, when illegal funds are moved through financial system for financing terrorism or related activities.

It is estimated that the extent of global money laundering ranges between USD 0.8 Tn to 2 Tn i.e. 2% to 5% of global GDP. As per global ML Index Tajikistan has highest score of 8.30, while Finland has the lowest score of 2.57 ranking 129. India stood at 68 rank with a score of 5.28.

B. Effects of Money Laundering

Following are the major effects of Money Laundering:

- Adverse impact on economy
- Risk of losing foreign investment
- Attracts anti-social elements

C. Extent of Terrorism

Terrorism has spread widely across the world. As per the Institute of Economic Peace study "Global Terrorism Index' 2018 due to terrorism deaths in 2017 were 18814 and its economic impact was estimated at USD 52 bn. In 46 countries the impact of terrorism was worse than in the preceding year though it was lower in 94 countries.

D. Money Laundering Process

In money laundering the starting point is illegal funds that are mostly in cash. For deployment in legal avenues it is inducted in financial system. The end result is legal funds. Typical money laundering process has three stages shown in Figure 1 on the next page.

It is not necessary that all three stages are used in all cases. Further, at placement stage cash may not be used in all cases. There are instances when illegal money is generated within the financial system itself.

In traditional money laundering process, it is easiest to detect money laundering during the placement stage. Next, at the layering stage also it is possible to detect it. At the integration stage it becomes rather too difficult to detect money laundering.

E. Terrorist Financing Process

For terrorist financing, funds are raised from variety of sources that could be spread over wider geographies. These are then moved to the place(s) of control. They may not be deployed wholly immediately. Typical terrorist financing process has the four stages shown in Figure 2 on the next page.

F. Differences between Money Laundering and Terrorist Financing

Money Laundering	Terrorist Financing
<ul style="list-style-type: none"> ➤ Source of funds is always legal. ➤ End use of funds is legal. ➤ Quantum of funds involved is larger. ➤ Objectives: <ul style="list-style-type: none"> – To disguise the source of funds – To park funds safely. – To earn returns on funds 	<ul style="list-style-type: none"> ➤ Source of funds can be legal and illegal both. ➤ End of use of funds is illegal i.e. terrorism. ➤ Quantum of funds involved is smaller most of the times. ➤ Objectives: <ul style="list-style-type: none"> – To hide usage of funds – To park funds safely. – To transfer funds secretly

Figure 1 – Money Laundering Stages

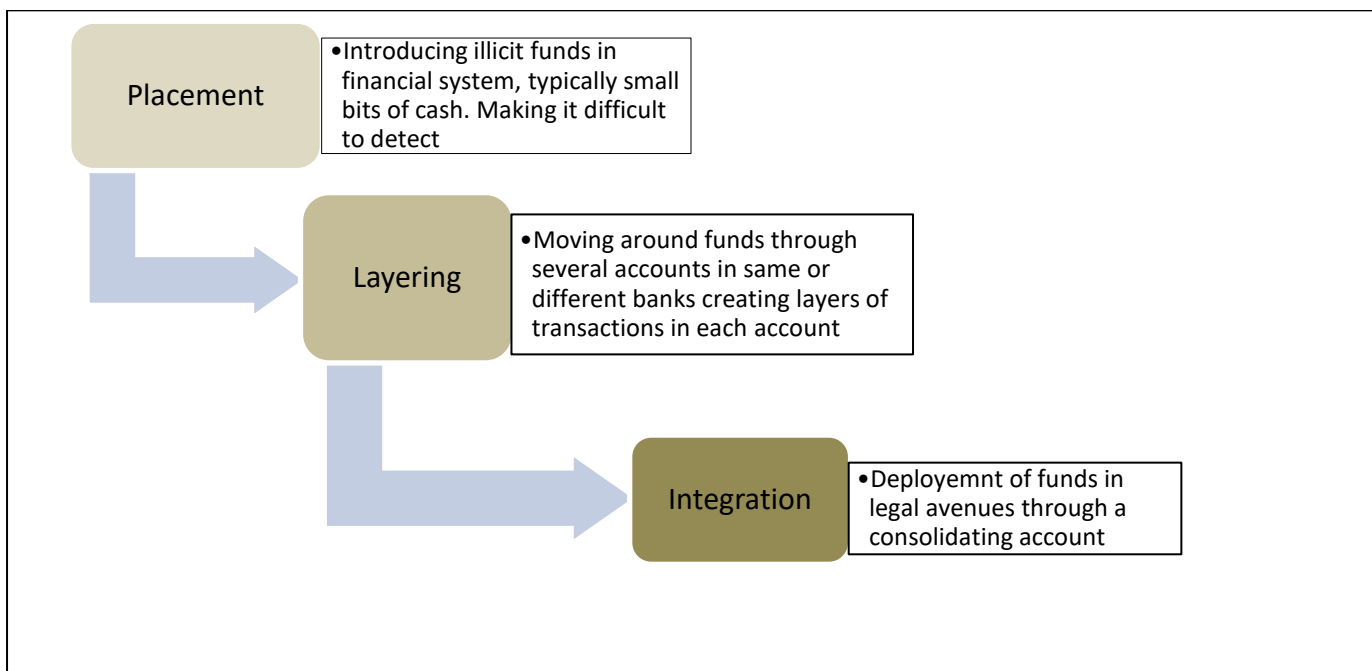
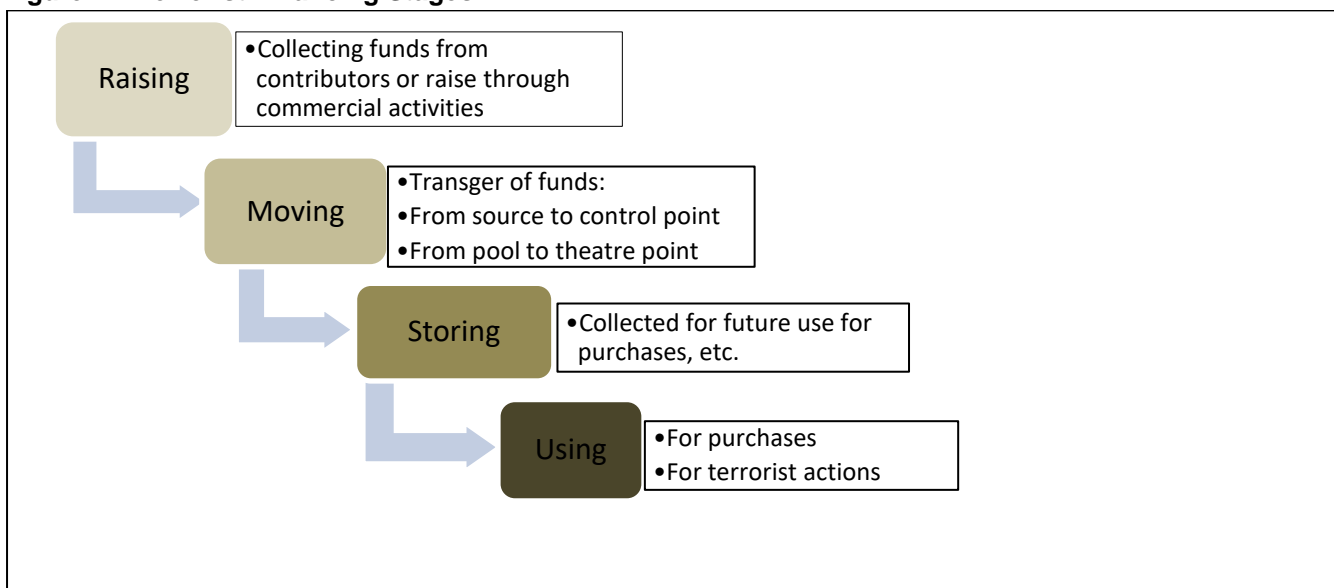


Figure 2 – Terrorist Financing Stages



II. International Norms

There are various international bodies that have issued guidance on anti-money laundering and combating financing terrorism related efforts. Some of the main forums are mentioned below.

A. Financial Action Task Force (FATF)

FATF is an inter-governmental body set up specifically to focus on money laundering and terrorist financing risks and evolve measures that need to be adopted to mitigate these risks. It has issued FATF international Standards for this purpose. These are extensive covering various aspects and are the guideposts for setting up of AML/CFT regime in various countries that are associated with FATF and also several other guidance papers related to

some of the major sectors and activities vulnerable to money laundering.

B. Regional Bodies (like APG, EAG)

There are several Regional Bodies that are playing similar role as FATF at the Regional level. These bodies are associated with FATF and work towards more effective implementation of FATF Standards by the jurisdictions within their region. These foster co-ordination among the jurisdictions at the regional level taking into account the socio-economic environment prevalent in the region.

Asia Pacific Group (APG) has issued several papers on AML measures like on Trade Based Money Laundering, and on Typologies.

Eurasian Group (EAG) has also issued several papers like Cybercrime and Money Laundering, tax Crimes and Money Laundering Typology, and various other typology reports.

C. Basle Committee on Banking Supervision (BCBS)

It has also issued guidelines on Customer Due Diligence, Accounts opening and Customer Identification, Wire Transfer and Money Laundering and Terrorist Financing Risk Management.

D. Wolfsberg Group

The Wolfsberg Group is an association of thirteen global banks which aims to develop frameworks and

guidance for the management of financial crime risks. It has issued Guidelines or Principles for the practices in several areas like Correspondent Banking, Terrorist Financing, Tax Evasion, etc.

E. FATF Standards

FATF had issued initially 40 Recommendations for prevention of money laundering that were later followed by 9 Special Recommendations on combating terrorist financing. In 2012, these were merged into 40 Standards. These cover various areas spanning from risk assessment, nature of legislation, role of finance sector and designated non finance businesses and professions, measures for specific activities or sectors, and international co-operation.

III. AML/ CFT Framework in India

India has adopted FATF Recommendations since their early stages. It had joined FATF initially as an Observer and was admitted as its member in 2010, after its implementation of FATF Recommendations was found to be satisfactory based on a joint evaluation undertaken by FATF and APG. India is also a member of two Regional bodies viz. APG and EAG.

A. Legislative Framework in India for AML/CFT

A specific legislation has been enacted related to Money Laundering. Provisions related to terrorism and terrorist financing have been incorporated in an existing law connected with unlawful activities. Besides, there are few other laws that also contain provisions that serve as control over money laundering. Following laws provide the legislative regime for AML/CFT measures:

- i) Prevention of Money Laundering Act / Prevention of Money Laundering (Maintenance of Records) Rules (PMLA/ PMLR)
- ii) Unlawful Activities Prevention Act (UAPA)
- iii) Regulatory Instructions/ Guidelines
- iv) Guidance by SROs (especially IBA)
- v) Foreign Contribution Regulation Act (FCRA)
- vi) Income Tax Act (IT Act)
- vii) Prohibition of Benami Transactions Act

B. Organizational Framework in India for AML/CFT

For mitigating money laundering and terrorist financing risks at various stages various agencies and organisations have been assigned different roles.

The roles played by these are briefly enumerated below.

- i) *Finance Ministry (Central Govt.):* It is responsible for proper legislation and for co-ordination with FATF and other international and multilateral agencies. It also supervises the functioning of FIU through the Economic Intelligence Council.
- ii) *Financial Intelligence Unit – India (FIU-IND):* This is a separate authority set up in pursuance of FATF Standards. Its role is to collect various types of transaction reports from finance sector players, and players in certain non-finance businesses, and analyse these. Based on the analysis, it provides information to one of the law enforcement agencies for further investigation as considered appropriate by it. It also monitors implementation of the provisions of PMLA by the business entities in various sectors, and provides guidance to them where required. It also co-ordinates with the sectoral regulators for the purpose of issuance of sectoral guidance related AML/ CFT Measures.
- iii) *Regulators:* Regulatory bodies like RBI, SEBI, OFRDA, IRDA issue specific guidelines for AML/ CFT measures for the specific sector. They also ensure that AML/ CFT aspects are also taken into account in any other regulations/ instructions issued by them covering various sectoral activities.
- iv) *Law Enforcement Agencies (LEAs):* These are responsible for investigation and prosecution related to various offences including money laundering and terrorist financing. They act upon the information received from FIU-IND about various suspicious transactions and take up the matter for investigation as appropriate.

Directorate of Enforcement (ED) is responsible for investigating Money Laundering offence. For terrorist financing offence, National Investigating Agency (NIA) looks into terrorism and terrorist financing offences. Besides, other investigating agencies connected with predicate offences are also connected with this. Some of these are Directorate Generals of Income Tax (Intelligence and Criminal Investigations) (DG) under Central Board of Direct Taxes (CBDT), Directorate of Revenue Intelligence (for Customs related), Central Economic Intelligence Bureau, Economic Offences Wing (EoW), Serious Frauds Office (SFIO), Central Bureau of Investigation,

Intelligence Bureau, Narcotics Control Bureau, Wildlife Crime Control Bureau,

- v) *Reporting Entities (RE's)*: The players in various financial sector areas like banking, insurance, mutual funds, capital market intermediaries, and also certain non-finance businesses and professions like real estate, jewelers, casino. They are required to follow certain procedure for due diligence of their customers, monitor transactions, and submit prescribed reports to FIU-IND. They play an important role of providing valuable leads on suspicious transactions carried out through them by customers. This information becomes the beginning point for the LEAs to start an investigation into a suspected criminal activity.

IV. Organizational Set-up in Bank/ FI

The obligations of a bank or financial institution under PMLA call for enterprise-wide responsibility. The scope of these provisions extends to cover all activities carried out by a bank/ financial institution. Secondly, these impact the processes related to customer onboarding, transaction execution and transaction monitoring significantly. Thirdly, the laws have placed the onus of compliance with the Boards and the senior management of the RE's.

- i) *Board/ Committee*: The overall responsibility of implementation of PMLA is with the Board. The board needs to ensure that the entity has put in place proper organisation set-up, processes, and control systems for this purpose. It should also monitor on ongoing basis through key parameters that the provisions are being complied in the course of business activities. For closer monitoring, the Board would require one of the Committees of the Board viz. Audit Committee of Board (ACB) (or Compliance Committee, if formed) to look into various aspects of compliance with PMLA.
- ii) *Chief Executive Officer (CEO)*: By virtue of his role, the CEO has the ultimate responsibility for compliance with the PMLA provisions at the execution level. He is responsible for having a proper KYC Policy, the required organisations set-up, monitoring that the necessary processes and control systems are put in place, and these are continuously evolved. Also, he needs to ensure that the entire organisation is sensitized regarding the obligations for KYC/ AML.
- iii) *Designated Director*: As per law, each RE is required to nominate one of the specified persons as the 'Designated Director' who will have the ultimate responsibility for compliance with PMLA. In case of banks/ FIs that are incorporated as a limited company, this may be one of the whole-

time directors. The Designated Director will have the responsibility for having a KYC Policy, ensuring proper organisation in place, and also its effective functioning. Where she is different from the CEO, she assists the CEO in fulfilment of the latter's responsibility.

- iv) *Principal Officer*: As per law, each RE has to appoint a Principal Officer who is responsible for submission of the prescribed reports and any other information called for to the Director, FIU-IND.
- v) *AML Team*: The Principal Officer is to be assisted by a Team of executives for the purpose of transaction monitoring, compilation of reports to FIU-IND, and submission of Reports to FIU. It will also collect, collate and prepare any other information called for by the FIU. Besides, it also assists in KYC Policy formulation and updation.
- vi) *Business/ Operations Teams*: These teams are responsible for ensuring that in their regular activities various requirements pertaining to customer due diligence, transaction due diligence, and transaction monitoring from AML/ CFT perspective are being observed. These aspects are also to be kept in view and built into when undertaking new product formulation, review of existing product, process designing/ reviewing, control systems formulation/ review.
- vii) *Branches*: The branch level staff and the front-office marketing staff also have significant role especially in customer due diligence and also in real time transaction scrutiny that are initiated by the customer during branch visit.
- viii) *Internal Audit/ Concurrent Audit*: This is a critical area for the focus of Internal Audit not only for audit of the AML Team, but also during the Audit of all business/ process teams. For certain critical

- aspects like KYC during new customer onboarding, concurrent audit may be put in place.
- ix) *Compliance Function*: Compliance function needs to cover this area in its review of policies, processes, procedures as also live test checks at the execution stage. It also needs to cover

completeness and quality of FIU reports being submitted.

It is also prescribed that periodically the entity should have its AML/CFT framework evaluated by an independent third party skilled in the area.

V. Legal & Regulatory Provisions – Salient Features

For banks and other financial services businesses regulated by the RBI the provisions related to AML/ CFT are contained in the following documents:

- i) Prevention of Money Laundering Act
- ii) Prevention of Money Laundering (Maintenance of Records) Rules
- iii) RBI Master Direction – Know Your Customer (KYC) Direction 2016

Salient features of these laws and regulations are enumerated below:

- ❖ Assessment of ML/ TF risks inherent in the business activities
- ❖ Customer due diligence at the time of onboarding for account-based relationship or at the time of undertaking specified transactions for a non-account holder
- ❖ Maintaining customer profile
- ❖ Risk categorization of customers and products/ services
- ❖ On-going diligence and periodical updation of customer profile
- ❖ Transaction monitoring for detection of suspicious transactions

- ❖ Submission of prescribed reports to FIU
- ❖ Specific provisions for select customers/ products

In respect of AML/ CFT related compliances banks/ FIs are subject to monitoring by two authorities viz. the RBI (or another sectoral Regulator) and the Director, FIU-IND. Hence any violation or non-compliance exposes to punitive measures by both these authorities. Non-compliance with the legal and regulatory provisions may attract following penal measures:

a) For the entity: Any or both the authorities may take any or more of the following actions against the entity:

- Issue a warning
- Issue direction to take certain measures and confirm compliance
- Impose monetary penalty

b) For individuals: The Director, FIU- IND may take any of the abovementioned actions against any errant officer/ employee of the entity.

VI. Customer Due Diligence

The primary objective of CDD and KYC requirements is to ascertain genuineness of the customer. This implies ascertaining the following:

- Genuine identity of the customer
- Customer is engaged in genuine activity

Customer due diligence has following main elements:

- i) Identifying customer: To establish identity and address of individuals through any of the Officially Valid Documents (OVDs) and verify the same. In case of entities, to establish their existence through any of the legal documents, any other official documents and/ or field verification. Also, to ascertain and identify the mandate holders (to obtain OVD) who act for the entity. Determining that these are not in any sanctions lists.
- ii) Identifying beneficial owners: For entity, to identify its beneficial owners (viz. the persons owning/ managing/ controlling the entity) and verify their identity (to obtain OVD). Beneficial

owners to be determined as per the prescribed criteria.

- iii) Identify Activity/ Source of funds: Ascertaining occupation, business activity, source of income, assets or source of wealth of the customer.
- iv) Other business/ financial aspects: Obtaining information about the normal level of financial turnover, business linkages viz. customers and suppliers, etc.

The KYC and other document requirements for different types of customers is given at Appendix.

Certain other aspects to be observed in respect of customers on boarded are:

- i) Preparing customer profiles containing information depending on the risk category of the customer
- ii) KYC exercise is required to be done at the customer level and not for individual customer

- level, for which Uniform Customer Identification Code is to be allotted to each customer.
- iii) Periodical updation is required to be done at prescribed periodicity at least i.e. 2/5/8 years for high/ medium/ low risk customers, and history is to be recorded.
 - iv) Relationship with certain customers is prohibited viz. whose identity cannot be established, who desires benami or anonymous accounts/ transactions or accounts/ transactions in fictitious names.
 - v) For financial inclusion, persons not having any OVD can be provided facility of Small Account with specified procedure and restrictions.
 - vi) PAN quoting and PAN validation for the prescribed transactions including account

- opening is mandatory. If the customer does not have PAN, Form 60 is to be obtained.
- vii) Wire transfers to contain complete information about the remitter (verified by the ordering bank) and the beneficiary's name and account number.

For some categories of customers viz. Self-help Groups and Foreign Portfolio Investors certain simplified procedures have been specified, For Foreign Students, subject to restrictions some dispensation has been provided for producing the local address proof, subject to restrictions. Politically Exposed Persons are determined as per the prescribed definition, and for these extensive due diligence requirements have been laid down, as also approval at a higher level has been stipulated.

VII. Customer Risk Categorisation

The requirements of KYC/ CDD and transaction monitoring for AML/ CFT are extensive, and are also resource intensive. To cover all the customers and transactions to the same degree is very onerous and will be cost prohibitive. With a view to more effective and efficient application of AML measures, Risk based approach has been prescribed. Banks and FI are required to carry out risk assessment of their customers and products/ services and categories them into different risk categories.

Risk from a customer is a function of various factors. Some of these are as follows:

- i) Constitution
- ii) Activity
- iii) Financial Status
- iv) Social Status
- v) Turnover
- vi) Linkages

Typically, customers are categorized in 3 categories, but if desired the categorization may be in to 5 categories – very high, high, medium, low and very low.

The due diligence measures can be calibrated depending on the risk category. High risk customers are to be subjected to Enhanced Due Diligence.

Some of the typical customers falling into high risk and medium risk categories are enumerated below.

High Risk
<ul style="list-style-type: none"> • Persons on Negative Lists • Politically Exposed Persons/ Non-Residents • Offshore businesses/ Entities - complex structures • Precious stones/ metals dealers • Arms/ Antique dealers • Non-profit organisations • High Net worth Individuals • Lawyers
Medium Risk
<ul style="list-style-type: none"> • Travel and Tour operators • Real Estate Agents • Travel Agents • Electronic goods merchants • Restaurants • Petrol dealers • Transport companies • Used card dealers

VIII. FIU – Reporting

There are in all five reports required to be submitted to FIU-IND. These fall into two categories:

- (a) Periodical Reports, (b) As and when report

A. Periodical Reports

The reporting entities are required to report undermentioned monthly reports to FIU-IND, by the 15th of the following month.

- (i) *Cash Transactions Report (CTR)*: To report all cash transactions of more than Rs.10 lac, and

integrally connected cash transactions of aggregate value of more than Rs.10 lac in the month. These include both receipt and payments, and are customer based and not account based. Thus, transactions in all accounts and for any product are to be included. In the report individual transactions of less than Rs.50,000/- are not included. Integrally connected means all receipts (or payments taken separately) during the month.

(ii) *Cross Border Wire Transfers Report (CBTR)*: All wire transfers of more than Rs. 5 lacs made into India or sent out of India. These include all remittances irrespective of their purpose. The origin and destination of funds are in different countries, irrespective of their route.

(iii) *Non-Profit Organization Transactions Report (NPR)*: All receipts of more than Rs.10 lacs by NPOs. These could be through any mode, and from any source domestic or cross-border.

(iv) *Counterfeit Currency Report (CCR)*: All transactions of any value involving use of counterfeit currency notes. Typically, these would be cash receipts, may be from account holders or from walk-in-customers. The report should be reconciled with reports submitted to the Police, RBI and National Crime Records Bureau.

B. As and when Report

The fifth report viz. Suspicious Transactions Report (STR) is a report that is required to be submitted as and when a suspicious transaction is detected. Salient features of STR are described below:

Transaction includes various types of transactions like:

- (i) opening of an account
- (ii) deposits, withdrawal, exchange or transfer in any currency (cash / cheque/ PO/ any instrument/ electronic / non-physical means)
- (iii) safety deposit box / safe deposit
- (iv) any fiduciary relationship
- (v) any payment made/ received for any contractual/ legal obligation
- (vi) any payment for games of chance/ casino
- (vii) establishing or creating a legal person or legal arrangement

Suspicious transaction is determined based on the following criteria:

- Seems to involve proceeds of a specified offence
- Seems to involve financing of terrorism related activities
- Unusual or unjustified complexity
- No economic rationale or bonafide purpose

STR is the key report for FIU-IND which is used by it for further transmission to the appropriate LEA. This in fact is the objective of entire AML regime. The details provided in the STR should be adequate for FIU-IND to determine that there indeed is a basis for suspecting some money laundering or terrorist financing, and also conclude the nature of predicate offence. This helps FIU-IND to decide to which LEA the STR should be directed. STR needs to be filed even for attempted transactions. STR is not a value-based but judgment-based report. STRs are confidential, and neither its contents nor the fact that STR has been filed should be divulged to any one or the customer.

Banks and FIs need to put in place appropriate organisations set-up; systematic processes for escalation, investigation, report generation/ compilation; and IT systems for detection of reportable transactions, and transactions likely to be suspicious.

For the purpose of determining suspicious transactions among innumerable transactions taking place daily, there is a need to put in place a rigorous mechanism. Essentially, the procedure is based on red flag indicators that are divided in two categories - manual and system-based. For system-based alerts, several rules are designed with appropriate threshold values. IT application is used for filtering all the transactions post-facto and throw up transactions that match the rules.