IMPORTANCE OF ANTI-MONEY LAUNDERING MEASURES AND EFFECTIVE KYC IN FINANCIAL TRANSACTIONS

Index

PREFACE

Initially, banks were encouraged and are now required to establish guidelines and procedures to identify potential money laundering schemes in order to file Suspicious Activity Reports with the government/regulatory authority. Money-laundering has acquired a global character that not only threatens security, but also compromises the stability, transparency and efficiency of financial systems. Money-laundering techniques are becoming more sophisticated and complex with each passing day.

Money laundering has become a pertinent problem worldwide threatening the stability of various regions by actively supporting and strengthening terrorist networks and criminal organizations. The links between money laundering, organized crime, drug trafficking and terrorism pose a risk to financial institutions globally. Across the world, banks and financial institutions are required to introduce and implement systems to prevent anti-social elements from using banking channels for money laundering. One of the most important tools used by banks to expose criminal activity has been to adopt "Know Your Customer" guidelines that help detect suspicious activity by account holders. Adoption of appropriate know-your-customer (KYC) procedures within individual banks is an essential part of risk management in banks, to safeguard the confidence and the integrity of banking systems.

This book provides the theoretical background on the subject and practical steps for banks implementing an AML/KYC regime in accordance with international standards. It explains the basic elements required to build an effective AML/KYC framework and summarizes the role of the employees in fighting money laundering.

This book would help in gaining a deeper knowledge and understanding on the various aspects of AML/KYC and will be useful to bankers, auditors, academicians and policy makers and persons dealing with banks and financial institutions.

1. INTRODUCTION

World over, the fight against money laundering and financing of terrorism has become the topmost priority. Money laundering poses a risk to the soundness and stability of financial institutions and financial systems, increased volatility of international capital flows, and a dampening effect on foreign direct investment. Protecting the integrity and stability of the international financial system, cutting off the resources available to terrorists, and making it more difficult for those engaged in crime to profit from their criminal activities are some of the measures taken in this regard.

Many of the methods applied by criminals to launder money or finance terrorism involve the use of the financial system to transfer funds. Financial institutions, in particular banks, are most vulnerable to abuse for that purpose. In order to protect themselves, it is essential that financial institutions have adequate control and procedures in place that enable them to know the person with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls.

1.1. What is a financial transaction?

A transaction is generally defined as a purchase, sale, loan, pledge, gift, transfer, delivery, other disposition, and with respect to a financial institution, a deposit, withdrawal, transfer between accounts, loan, exchange of currency, extension of credit, purchase or sale safe-deposit box, or any other payment, transfer or delivery by, through or to a financial institution.

Hence a financial transaction can be defined as a transaction which affects interstate or foreign commerce and involves the movement of funds by wire or by other means; involves the use of a monetary instrument; or involves the transfer of title to real property, a vehicle, a vessel or an aircraft; or involves the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce.

1.2. What is a Financial Institution?

Financial institution is an establishment that focuses on dealing with financial transactions, such as investments, loans and deposits. Conventionally, financial institutions are composed of organizations such as banks, trust companies, insurance companies and investment dealers. Almost everyone has to deal with a financial institution on a regular basis. Everything from depositing money to taking out loans and exchange currencies must be done through financial institutions.

According to **Section 2(1)(l) of Prevention of Money-Laundering Act, 2002**, "Financial institution" means a financial institution as defined in clause (*c*) of section 45-I of the Reserve Bank of India Act, 1934 and includes a chit fund company, a housing finance institution, an authorised person, a payment system operator, a non-banking financial company and the Department of Posts in the Government of India.

According to **Section 45-I(c) of the Reserve Bank of India Act, 1934** ''financial institution'' means any non-banking institution which carries on as its business or part of its business any of the following activities, namely:–

(i) the financing, whether by way of making loans or advances or otherwise, of any activity other than its own:

(ii) the acquisition of shares, stock, bonds, debentures or securities issued by a Government or local authority or other marketable securities of a like nature:

(iii) letting or delivering of any goods to a hirer under a hire-purchase agreement as defined in clause (c) of section 2 of the Hire-Purchase Act, 1972:

(iv) the carrying on of any class of insurance business;

(v) managing, conducting or supervising, as foreman, agent or in any other capacity, of chits or kuries as defined in any law which is for the time being in force in any State, or any business, which is similar thereto;

(vi) collecting, for any purpose or under any scheme or arrangement by whatever name called, monies in lumpsum or otherwise, by way of subscriptions or by sale of units, or other instruments or in any other manner and awarding prizes or gifts, whether in cash or kind, or disbursing monies in any other way, to persons from whom monies are collected or to any other person, but does not include any institution, which carries on as its principal business,–

(a) agricultural operations; or

(aa) industrial activity; or

(b) the purchase or sale of any goods (other than securities) or the providing of any services; or

(c) the purchase, construction or sale of immovable property, so however, that no portion of the income of the institution is derived from the financing of purchases, constructions or sales of immovable property by other persons.

[Explanation.– For the purposes of this clause, ‘‘industrial activity’’ means any activity specified in sub-clauses (i) to (xviii) of clause (c) of section 2 of the Industrial Development Bank of India Act, 1964;]

According to the **Financial Action Task Force (FATF)**, financial institutions mean any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1) Acceptance of deposits and other repayable funds from the public.
2) Lending.
3) Financial leasing.
4) Money or value transfer services.
5) Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6) Financial guarantees and commitments.
7) Trading in:

a. money market instruments (cheques, bills, certificates of deposits, derivatives etc.);

b. foreign exchange;

c. exchange, interest rate and index instruments;

d. transferable securities

e. commodity futures trading.

8) Participation in securities issues and the provision of financial services related to such issues.

9) Individual and collective portfolio management.

10) Safekeeping and administration of cash or liquid securities on behalf of other persons.

11) Otherwise investing, administering or managing funds or money on behalf of other persons.

12) Underwriting and placement of life insurance and other investment related insurance.

13) Money and currency changing.

This also captures private banking. This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting). This does not extend to financial leasing arrangements in relation to consumer products. This does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. This applies both to insurance undertakings and to insurance intermediaries (agents and broker).

1.3. How financial institutions are used for money laundering?

Financial institutions can be involved in financial crime in three ways - as victim, as perpetrator, or as an instrumentality.

Under the first category, financial institutions can be subject to different types of fraud including, e.g., misrepresentation of financial information, embezzlement, check and credit card fraud, securities fraud, insurance fraud, and pension fraud. Under the second (less common) category, financial institutions can commit different types of fraud on others, including, e.g., the sale of fraudulent financial products, self dealing, and misappropriation of client funds. In the third category are instances where financial institutions are used to keep or transfer funds, either wittingly or unwittingly, that are themselves the profits or proceeds of a crime, regardless of whether the crime is itself financial in nature. One of the most important examples of this third category is money laundering. Financial institutions can be used as an instrumentality to keep or transfer the proceeds of a crime. In fact, financial institutions are at the forefront of the battle against the money launderers.

2. WHAT IS MONEY LAUNDERING?

According to Section 3 of Prevention of Money Laundering Act, 2002 - 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 will be guilty of offence of money-laundering.

Financial Action Task Force on Money Laundering (FATF) defines money laundering as "the processing of criminal proceeds to disguise their illegal origin in order to legitimize the ill-gotten gains of crime."

Money laundering is frequently referred to as a financial crime. It is generally defined as "transferring illegally obtained money or investments through an outside party to conceal the true source." This activity may prevent law enforcement from uncovering or confiscating the proceeds of crime, or using the proceeds as evidence in a criminal prosecution. Such processing may involve disguising the beneficial owner of either the actual criminal proceeds or of other property that might be subject to confiscation. Money laundering can be done with or without the knowledge of the financial institution or counterparty to financial transactions, although to be guilty of the crime of money laundering, actual or implied knowledge is required.

The number and variety of transactions used to launder money has become increasingly complex, often involving numerous financial institutions from many jurisdictions, and increasingly using non-bank financial institutions. In addition laundered proceeds may not be cash but other financial instruments. Also, the use of non-financial businesses and markets for laundering appears to be increasing, including not only illegitimate institutions such as shell companies created as laundering instrumentalities, but legitimate companies where illicit funds are intermingled with legitimate funds.

Money laundering methods are diverse and are constantly evolving. They range from trade-related operations to on-line banking. Money launderers may also operate outside financial systems, for example, through alternative remittance systems. Other financial crimes can be associated with, or exist in parallel with, money laundering, for example, corruption, fraud, or

the control of a financial institution by organized crime. Upon the receipt of criminal proceeds, criminals may seek to launder them through the financial system. This, in turn, may also require a series of fraudulent activities such as counterfeiting invoices and the corrupting of bank employees. Thus, a whole chain of criminal or illegal activities may culminate in the flow of criminal money through the financial system.

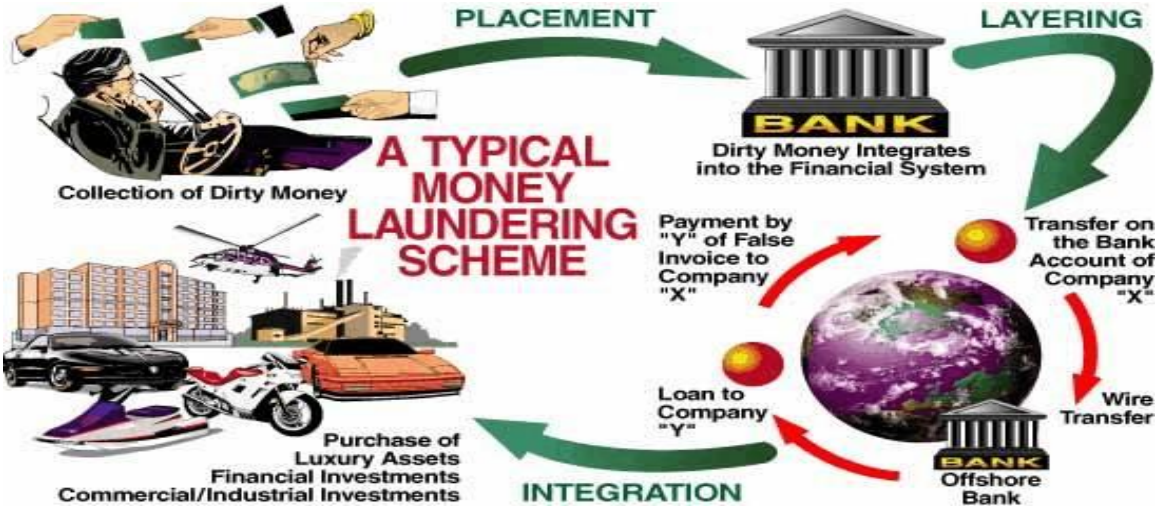
2.1. Why is money laundered?

There are several reasons why people launder money. These include:

- **hiding wealth**: criminals can hide illegally accumulated wealth to avoid its seizure by authorities;
- **avoiding prosecution**: criminals can avoid prosecution by distancing themselves from the illegal funds;
- **evading taxes**: criminals can evade taxes that would be imposed on earnings from the funds;
- **increasing profits**: criminals can increase profits by reinvesting the illegal funds in businesses;
- **becoming legitimate**: criminals can use the laundered funds to build up a business and provide legitimacy to this business.

2.2. Money Laundering process and methods

Money laundering is not a single act but is in fact a process that is accomplished in three basic steps. These steps can be taken at the same time in the course of a single transaction, but they can also appear in well separable forms one by one as well.



i. **Placement**:

The Money Launderer, who is holding the money generated from criminal activities, introduces the illegal funds into the financial systems. This might be done by breaking up large amount of cash into less conspicuous smaller sums which are deposited directly into a Bank Account or by purchasing a series of instruments such as Cheques, Bank Drafts etc., which are then collected and deposited into one or more accounts at another location.

Most common ways for Placement are –

- Deposit cash into one or more bank accounts in broken up amounts in several branches in one financial institution or different financial institutions.
- Purchase money orders, bank drafts and other financial instruments.
- Commingle the funds with legitimate ones.
- Exchange the funds into foreign currencies through a private foreign exchange dealer.
- Exchange large denominations for smaller ones.
- Cash purchase of a security or a form of an insurance contract.

ii. **Layering**:

The second stage of Money Laundering is layering. In this stage, the Money Launderer typically engages in a series of continuous conversions or movements of funds, within the financial or banking system by way of numerous accounts, so as to hide their true origin and to distance them from their criminal source. The Money Launderer may use various channels for movement of funds, like a series of Bank Accounts, sometimes spread across the globe, especially in those jurisdictions which do not co–operate in anti Money Laundering investigations.

Segregation of funds from its illegal origin -

- Purchase other securities, insurance contracts or other easily transferable investment instruments and then sold yet through another institution.
- Transfer through cheque, money order or bearer bond.
- Wire or remit the funds to various accounts and jurisdictions and disguise the transfer as a payment for goods or services.

iii. **Integration**:

Having successfully processed his criminal profits through the first two stages of Money Laundering, the Launderer then moves to this third stage in which the funds reach the legitimate economy, after getting inseparably mixed with the legitimate money earned through legal sources of income. The Money Launderer might then choose to invest the funds into real estate, business ventures & luxury assets, etc. so that he can enjoy the laundered money, without any fear of law enforcement agencies.

The above three steps may not always follow each other. At times, illegal money may be mixed with legitimate money, even prior to placement in the financial system. In certain cash rich businesses, like Casinos (Gambling) and Real Estate, the proceeds of crime may be invested without entering the mainstream financial system at all.

Money-laundering Methods

These are the common methods under each stage of money laundering.

Under Placement Stage

- *Currency Smuggling* – This is the physical illegal movement of currency and monetary instruments out of a country. The various methods of transport do not leave a discernible audit trail.

- *Bank Complicity* – This is when a financial institution, such as banks, is owned or controlled by unscrupulous individuals suspected of conniving with drug dealers and other organised crime groups. This makes the process easy for launderers. The complete liberalisation of the financial sector without adequate checks also provides leeway for laundering.

- *Currency Exchanges* – In a number of transitional economies the liberalisation of foreign exchange markets provides room for currency movements and as such laundering schemes can benefit from such policies.

- *Securities Brokers* – Brokers can facilitate the process of money laundering through structuring large deposits of cash in a way that disguises the original source of the funds.

- *Blending of Funds* – The best place to hide cash is with a lot of other cash. Therefore, financial institutions may be vehicles for laundering. The alternative is to use the money from illicit activities to set up front companies. This enables the funds from illicit activities to be obscured in legal transactions.

- *Asset Purchase* – The purchase of assets with cash is a classic money laundering method. The major purpose is to change the form of the proceeds from conspicuous bulk cash to some equally valuable but less conspicuous form.

Under Layering Stage

- *Cash converted into Monetary Instruments* – Once the placement is successful within the financial system by way of a bank or financial institution, the proceeds can then be converted into monetary instruments. This involves the use of banker's drafts and money orders.

- *Material assets bought with cash then sold* – Assets that are bought through illicit funds can be resold locally or abroad and in such a case the assets become more difficult to trace and thus seize.

Under Integration Stage

- *Property Dealing* – The sale of property to integrate laundered money back into the economy is a common practice amongst criminals. For instance, many criminal groups use shell companies to buy property; hence proceeds from the sale would be considered legitimate.
- *Front Companies and False Loans* – Front companies that are incorporated in countries with corporate secrecy laws, in which criminals lend themselves their own laundered proceeds in an apparently legitimate transaction.
- *Foreign Bank Complicity* – Money laundering using known foreign banks represents a higher order of sophistication and presents a very difficult target for law enforcement. The willing assistance of the foreign banks is frequently protected against law enforcement scrutiny. This is not only through criminals, but also by banking laws and regulations of other sovereign countries.
- *False Import/Export Invoices* – The use of false invoices by import/export companies has proven to be a very effective way of integrating illicit proceeds back into the economy. This involves the overvaluation of entry documents to justify the funds later deposited in domestic banks and/or the value of funds received from exports.

2.3. Factors that facilitated the explosion of money laundering

1. The globalisation of markets and financial flows, most evident in the advent of the Internet. The creation of the single market means that money can now travel in nanoseconds, meaning that multiple jurisdiction leaps are made effortlessly on a daily basis.

2. Deregulation of financial markets has bought with it no consistency or coherence in respect of anti-money laundering regulations; simultaneously today's global market place has bought with it very few if any restrictions.
3. Globalisation implies global competition, meaning more competitors and increasing pressure to deliver profits. The proceeds of crime are massive meaning that the people who control them can yield great influence with legitimate businesses, which are hungry, sometimes even desperate for profits.

2.4. The Internet and Money Laundering

As a result of international clampdown against money laundering, criminals have started to look for new tools and mechanisms to hide the origins of their ill-gotten gains and to channel them from one location to another. What they want is a way to launder their illicit proceeds that is quick, discrete, secure and global. A near perfect tool meeting all these conditions is the internet: an extremely swift, relatively secure, almost anonymous and truly global instrument. Due to its decentralised structure, the internet has increasingly become the mechanism of choice of many criminals to channel funds from one global location to another, sometimes in mere minutes and, if handled professionally, without leaving too many traces. Although most of the amounts thus shifted are currently thought to be still relatively small compared to the overall volume of funds laundered, the practice of using the internet as a tool to hide the origins of illicit funds is growing fast. And as criminals and terrorists across the world get increasingly cyber-savvy, they make more and more frequently use of the above mentioned advantages of the internet and thus succeed in often staying several steps ahead of most law enforcement officers, who are only gradually starting to get to grips with the virtually unlimited possibilities of the World Wide Web.

2.5. Combat cyber-laundering

All institutions involved in preventing and combating money laundering and terrorist financing, especially supervisory and law enforcement bodies, urgently need to strengthen their IT

knowledge to keep up pace with criminals across the world. This includes increased training and, if needed, the hiring of former hackers.

Criminals and terrorists can often operate largely anonymously due to lax enforcement of due diligence, in particular in areas outside the financial industry. It is therefore necessary to introduce better ID checks with new financial instruments (e.g. prepaid storage cards), especially outside the financial sector. This could help reduce the use of anonymous payments.

Cyber-savvy users can relatively easily avoid the tracking of their online identity by using proxy servers and anonymous software. Although a certain degree of online anonymity is acceptable, especially in politically delicate regions of the world, financial operations should never be conducted anonymously. Hence better IP tracking to prevent criminals from hiding their online identities are required.

Criminals can easily exploit the lack in international co-operation by moving from country to country. Therefore better international co-operation and co-ordination to prevent and combat money laundering and terrorist financing is required. National and international efforts and instruments aimed at combating online money laundering and terrorist financing, for example by allowing for faster exchange of information and speeding up requests for mutual legal assistance should be strengthened.

3. OVERVIEW OF ANTI-MONEY LAUNDERING LAWS IN INDIA

In India money laundering is popularly known as Hawala transactions. It gained popularity during early 90's when many of the politicians were caught in its net. Hawala is an alternative or parallel remittance system. The Hawala Mechanism facilitated the conversion of money from black into white. "Hawala" is an Arabic word meaning the transfer of money or information between two persons using a third person. The system dates to the Arabic traders as a means of avoiding robbery. It predates western banking by several centuries.

The Government of India is committed to tackle the menace of Money Laundering and has always been part of the global efforts in this direction. India is signatory to the following UN Conventions, which deal with Anti Money Laundering / Countering the Financing of Terrorism :

1. International Convention for the Suppression of the Financing of Terrorism (1999);
2. UN Convention against Transnational Organized Crime (2000); and
3. UN Convention against Corruption (2003)

In pursuance to the political Declaration adopted by the special session of the United Nations General Assembly (UNGASS) held on 8th to 10th June 1998 (of which India is one of the signatories) calling upon member States to adopt Anti Money Laundering Legislation & Programme, the Parliament enacted a special law called the 'Prevention of Money Laundering Act, 2002' (PMLA 2002).

Before the enactment of the Prevention of Money-Laundering Act, 2002, the following statutes addressed inadequately the issue of money laundering—

- The Conservation of Foreign Exchange and Prevention of Smuggling Activities Act, 1974
- The Income Tax Act, 1961
- The Benami Transactions (Prohibition) Act, 1988
- The Indian Penal Code and Code of Criminal Procedure, 1973
- The Narcotic Drugs and Psychotropic Substances Act, 1985

- The Prevention of Illicit Traffic in Narcotic Drugs and Psychotropic Substances Act, 1988

This was not sufficient to tackle the growing menace of money laundering in India. In view of the urgent need for the enactment of a comprehensive legislation inter alia for preventing money laundering and connected activities, confiscation of proceeds of crime, setting up of agencies and mechanisms for coordinating measures for combating money-laundering etc., the PML Bill was introduced in the Lok Sabha on 4th August, 1998, which ultimately was passed on 17th January 2003.

The Prevention of Money-Laundering Act, 2002 (PMLA 2002) and the Rules notified thereunder came into effect on July 1, 2005. The Prevention of Money-Laundering Act, 2002 consists of ten chapters containing 75 sections and one Schedule. Amendments were made to this Act vide The Prevention of Money-laundering (Amendment) Act, 2005 (20 of 2005), Prevention of Money-laundering (Amendment) Act, 2009 (21 of 2009) and Prevention of Money laundering-(Amendment) Act, 2012 (2 of 2013).

The object of the Act is to prevent money-laundering and to provide for confiscation of property derived from, or involved in, money-laundering and to punish those who commit the offence of money laundering. The Act extends to the whole of India including the state of Jammu and Kashmir.

The following rules have been notified under the Prevention of Money Laundering Act, 2002—

(1) The Prevention of Money-laundering (the Manner of forwarding a copy of the Order of Provisional Attachment of Property along with the Material, and copy of the Reasons along with the Material in respect of Survey, to the Adjudicating Authority and its period of Retention) Rules, 2005 — Notification No. GSR 442(E), dated 01-07-2005

(2) The Prevention of Money-Laundering (Receipt and Management of Confiscated Properties) Rules, 2005 — Notification No. GSR 443(E), dated 01-07-2005

(3) The Prevention of Money-laundering (Maintenance of Records) Rules, 2005 - Notification No. GSR 444 (E), dated 01-07-2005.

(4) The Prevention of Money-laundering (Forms, Search and Seizure and the Manner of Forwarding the Reasons and Material to the Adjudicating Authority, Impounding and Custody of Records and the Period of Retention) Rules, 2005 — Notification No. GSR 445 (E), dated 01-07-2005.

(5) The Prevention of Money-laundering (the Forms and the Manner of Forwarding a Copy of Order of Arrest of a Person along with the Material to the Adjudicating Authority and its period of Retention) Rules, 2005 — Notification No. GSR 446(E), dated 01-07-2005.

(6) The Prevention of Money-laundering (the Manner of Forwarding a Copy of the Order of Retention of Seized Property along with the Material to the Adjudicating Authority and the period of its Retention) Rules, 2005 — Notification No. GSR 447(E), dated 01-07-2005.

(7) The Prevention of Money-laundering (Manner of Receiving the Records authenticated Outside India) Rules, 2005 — Notification No. GSR 448(E), dated 1-7-2005.

(8) The Prevention of Money-laundering (Appeal) Rules, 2005 — Notification No. GSR 449(E), dated 1-7-2005.

(9) The Prevention of Money-laundering (appointment and conditions of service of chairperson and members of adjudicating authorities) Rules, 2007 — Notification number GSR 520(E), dated 1-8-2007.

(10) The Prevention of Money-laundering (appointment and conditions of service of chairperson and members of Appellate Tribunal) Rules, 2007 — Notification number GSR 519(E), dated 1-8-2007.

(11) The Prevention of Money-laundering (Salaries, Allowances and other Conditions of The employees of Appellate Tribunal) Rules,2008 — Notification number GSR 430(E), dated 5-6-2008

(12) The Prevention of Money-laundering (Issuance of Provisional Attachment Order) Rules, 2013 – Notification number GSR 557(E), dated 19-8-2013

(13) The Prevention of Money-laundering (Taking Possession of Attached or Frozen Properties confirmed by the Adjudicating Authority) Rules, 2013 – Notification number GSR 558(E), dated 19-8-2013

(14) The Goa Anti Money Laundering and Financing of Terrorism Guidelines, 2013

4. ANTI-MONEY LAUNDERING MEASURES IN FINANCIAL TRANSACTIONS

Anti-money laundering (AML) is a term mainly used in the financial and legal industries to describe the legal controls that require financial institutions and other regulated entities to prevent, detect, and report money laundering activities. Anti-money laundering guidelines came into prominence globally as a result of the formation of the Financial Action Task Force (FATF) and the promulgation of an international framework of anti-money laundering standards. These standards began to have more relevance in 2000 and 2001, after FATF began a process to publicly identify countries that were deficient in their anti-money laundering laws and international cooperation, a process colloquially known as "name and shame".

An effective AML program requires a jurisdiction to have criminalized money laundering, give the relevant regulators and police - the powers and tools to investigate; be able to share information with other countries as appropriate; and require financial institutions to identify their customers, establish risk-based controls, keep records, and report suspicious activities.

The effective functioning of financial markets relies heavily on the expectation that high professional, legal, and ethical standards are observed and enforced. A reputation for integrity, soundness, honesty, adherence to standards and codes is one of the most valued assets by investors, financial institutions, and jurisdictions. Various forms of financial system abuse may compromise financial institutions' and jurisdictions' reputation, undermine investors' trust in them, and therefore weaken the financial system. The important link between financial market integrity and financial stability is underscored in the Basel Core Principles for Effective Supervision and in the Code of Good Practices on Transparency in Monetary and Financial Policies, particularly those principles and codes that most directly address the prevention, uncovering, and reporting of financial system abuse, including financial crime, and money laundering.

Money laundering may have other negative macroeconomic consequences. For example, it could compromise bank soundness with potentially large fiscal liabilities, lessen the ability to attract foreign investment, and increase the volatility of international capital flows and exchange rates.

4.1. Applicability of anti-money laundering laws

Anti-money laundering laws will be applicable to every individual or entity engaged in financial transactions.

Sec.2(1)(ha) of Prevention of Money-Laundering Act, 2002 (inserted by Prevention of Money-Laundering (Amendment) Act, 2012) defines "**Client"** as a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who engaged in the transaction or activity, is acting.

According to Sec.2(1)(s) of Prevention of Money-Laundering Act, 2002 "**person**" includes—

(*i*)an individual,

(*ii*)a Hindu undivided family,

(*iii*)a company,

(*iv*)a firm,

(*v*)an association of persons or a body of individuals, whether incorporated or not,

(*vi*)every artificial judicial person not falling within any of the preceding sub clauses, and

(*vii*)any agency, office or branch owned or controlled by any of the above persons mentioned in the preceding sub-clauses.

According to Sec.2(1)(wa) of Prevention of Money-Laundering Act, 2002 (inserted by Prevention of Money-Laundering (Amendment) Act, 2012) "**Reporting entity**" means a banking company, financial institution, intermediary or a person carrying on a designated business or profession.

"**Banking company**" means a banking company or a co-operative bank to which the Banking Regulation Act, 1949 (10 of 1949) applies and includes any bank or banking institution referred to in section 51 of that Act. (Sec.2(1)(e) of Prevention of Money-Laundering Act, 2002)

"**Financial institution**" means a financial institution as defined in clause (*c*) of section 45-I of the Reserve Bank of India Act, 1934 and includes a chit fund company, a housing finance institution, an authorised person, a payment system operator, a non-banking financial company and the Department of Posts in the Government of India. (Sec.2(1)(l) of Prevention of Money-Laundering Act, 2002)

According to Sec.2(1)(n) of Prevention of Money-Laundering Act, 2002 (inserted by Prevention of Money-Laundering (Amendment) Act, 2012), "**Intermediary**" means –

(*i*) a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser or any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992; or

(*ii*) an association recognised or registered under the Forward Contracts (Regulation) Act, 1952 or any member of such association; or

(*iii*) intermediary registered by the Pension Fund Regulatory and Development Authority; or

(*iv*)a recognised stock exchange referred to in clause (*f*) of section 2 of the Securities Contracts (Regulation) Act, 1956

"**Person carrying on designated business or profession**" means,—

(*i*) a person carrying on activities for playing games of chance for cash or kind, and includes such activities associated with casino;

(*ii*) a Registrar or Sub-Registrar appointed under section 6 of the Registration Act, 1908, as may be notified by the Central Government;

(*iii*) real estate agent, as may be notified by the Central Government;

(*iv*) dealer in precious metals, precious stones and other high value goods, as may be notified by the Central Government;

(*v*) person engaged in safekeeping and administration of cash and liquid securities on behalf of other persons, as may be notified by the Central Government; or

(*vi*) person carrying on such other activities as the Central Government may, by notification, so designate, from time to time. (Sec.2(1)(sa) of Prevention of Money-Laundering Act, 2002 (inserted by Prevention of Money-Laundering (Amendment) Act, 2012

4.2. Anti-money laundering measures prescribed under PMLA, 2002

Some of the anti-money laundering measures prescribed under the Prevention of Money Laundering Act, 2002 are –

- ✓ Various obligations have been imposed on reporting entities under Sec.12 of PMLA.
- ✓ Maintenance of record of all transactions for a period of 5 years from the date of transaction between a client and the reporting entity.
- ✓ Furnishing of information to authorities within the prescribed time.
- ✓ Verification of identity of clients.
- ✓ Identification of beneficial owners, if any.
- ✓ Maintenance of record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients for a period of five years after the business relationship between a client and the reporting entity has ended or the account has been closed, whichever is later.
- ✓ Maintenance of confidentiality of information.

All these information will help the authorities in identifying the sequence of any illegal activities.

"Reporting entity" means a banking company, financial institution, intermediary or a person carrying on a designated business or profession.

If the Director, in the course of any inquiry, finds that a a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations contained in section 12, then, without prejudice to any other action that may be taken under any other provisions of the Act, he may, issue a warning in writing; or direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or by an order, impose a monetary penalty on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure.

4.2.1. Maintenance of Records

Section 12(1)(*a*) of the Prevention of Money Laundering Act, 2002 makes it mandatory for every reporting entity to maintain a record of all transactions, including information relating to transactions whether attempted or executed so as to enable it to reconstruct individual transactions. The procedure for maintenance and retention of records are covered under the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 which was last amended by the Prevention of Money-Laundering (Maintenance of Records) Amendment Rules, 2013.

1) Records of transactions to be maintained

The following records should be maintained—

(1) all cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;

(2) all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month;

(3) all transactions involving receipts by non-profit organisations of value more than rupees ten lakh, or its equivalent in foreign currency;

(4) 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;

(5) all suspicious transactions whether or not made in cash and by way of—

(*a*) deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of:

(*i*) cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or

(*ii*) travellers cheques, or

(*iii*) transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts, or

(*iv*) any other mode in whatsoever name it is referred to

(*b*) credits or debits into or from any non-monetary accounts such as d-mat account, security account in any currency maintained by the banking company, financial institution and intermediary, as the case may be;

(*c*) money transfer or remittances in favour of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by any of the following—

(*i*) payment orders, or

(*ii*) cashiers cheques, or

(*iii*) demand drafts, or

(*iv*) telegraphic or wire transfers or electronic remittances or transfers, or

(*v*) internet transfers, or

(*vi*) Automated Clearing House remittances, or

(*vii*) lock box driven transfers or remittances, or

(*viii*) remittances for credit or loading to electronic cards, or

(*ix*) any other mode of money transfer by whatsoever name it is called;

(*d*) loans and advances including credit or loan substitutes, investments and contingent liability by way of—

(*i*) subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitized participation, inter bank participation or any other investments in securities or the like in whatever form and name it is referred to, or

(*ii*) purchase and negotiation of bills, cheques and other instruments, or

(*iii*) foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called, or

(*iv*) letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/or credit support.

(*e*) collection services in any currency by way of collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to.

(6) All cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India;

(7) All purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.

2) Information in the records

Apart from the records of transactions to be maintained, the records should also contain the following information -

(1) The nature of the transaction(s);

(2) the amount of the transaction and the currency in which it was denominated;

(3) the date on which the transaction was conducted; and

(4) the parties to the transaction.

3) Procedure and manner of maintaining information

Every reporting entity should maintain information in respect of transactions with its clients in accordance with the procedure and manner as may be specified by its Regulator, from time to time. Every reporting entity should evolve an internal mechanism for maintaining such information in such form and at such intervals as may be specified by its Regulator from time to time. It is the duty of every reporting entity, its designated director, officers and employees to observe the procedure and manner of maintaining information as specified by its Regulator.

4.2.2. Furnishing of Information

Section 12(1)(*b*) of the Prevention of Money Laundering Act, 2002, makes it mandatory for every reporting entity to furnish to the Director within the prescribed time, information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed.

1) Procedure and manner of furnishing information

- Every reporting entity should communicate to the Director (FIU-IND) the name, designation and address of the Designated Director and the Principal Officer.
- The Principal Officer should furnish the information regarding nature and value of transactions to the Director on the basis of information available with the reporting entity. A copy of such information should be retained by the Principal Officer for the purposes of official record.
- Every reporting entity should evolve an internal mechanism having regard to any guidelines issued by regulator, for detecting the transactions like cash transactions, suspicious transactions etc. and for furnishing information about such transactions in such form as may be directed by its Regulator.

- It is the duty of every reporting entity, its designated director, officers and employees to observe the procedure and the manner of furnishing information as specified by its Regulator.

2) Reports prescribed under PMLA, 2002

The Prevention of Money laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 require every reporting entity to furnish the following reports:

- Cash Transaction reports (CTRs)
- Suspicious Transaction Reports (STRs)
- Counterfeit Currency Reports (CCRs)
- Non Profit Organisation Transaction reports (NTRs)

3) Due dates for furnishing information to the Director (FIU-IND)

Description	**Due Date**
All **cash transactions** of the value of more than Rupees Ten lakhs or its equivalent in foreign currency	Every month by the 15th day of the succeeding month
All **series of cash transactions** integrally connected to each other which have been individually valued below Rupees Ten lakhs 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 Ten lakh rupees or its equivalent in foreign currency	
All transactions involving receipts by **non-profit organizations** of value more than Rupees Ten lakhs or its equivalent in foreign currency	
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 for facilitating the transactions	
All **cross border wire transfers** of the value of more than Five Lakh Rupees or its equivalent in foreign currency where either the origin or destination of fund is in India	
All **suspicious transactions** whether or not made in cash to be informed promptly writing or by fax or by electronic mail to the Director	Not later than seven working days on being satisfied that the transaction is suspicious
All purchase and sale by any person **of immovable property** valued at Fifty Lakh Rupees or more that is registered by the reporting entity	Every quarter by the 15th day of the month succeeding the quarter

The Principal Officer of a reporting entity should furnish the information in respect of the above mentioned transactions to the Director (FIU-IND). Delay of each day in not reporting a transaction or delay of each day in rectifying a mis-reported transaction beyond the time limit as specified above will constitute a separate violation.

4) Cash Transaction Reports

Cash transaction reports refer to:

- All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency.

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

Cash Transaction Reports are to be reported on a monthly basis by the 15th day of the month following the month of transaction. A Cash Transaction Report covers details of account, related persons and transactions for a month in a bank account.

5) Suspicious Transaction Reports

Suspicious transaction means a transaction whether or not made in cash which, to a person acting in good faith:

(*a*) gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or

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

(*c*) appears to have no economic rationale or bona fide purpose; or

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

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.

Suspicious Transaction Reports are required to be reported by the principal officer within 7 working days on being satisfied that the transaction is suspicious. Suspicious Transaction Reports will include details of all accounts, transactions, individuals and legal persons/entities related to suspicious transaction.

Examples of suspicious transactions for a banking company

Identity of client

- False identification documents
- Identification documents which could not be verified within reasonable time

- Accounts opened with names very close to other established business entities

Background of client

- Suspicious background or links with known criminals

Multiple accounts

- Large number of accounts having a common account holder, introducer or authorized signatory with no rationale
- Unexplained transfers between multiple accounts with no rationale

Activity in accounts

- Unusual activity compared with past transactions
- Sudden activity in dormant accounts
- Activity inconsistent with what would be expected from declared business

Nature of transactions

- Unusual or unjustified complexity
- No economic rationale or *bona fide* purpose
- Frequent purchases of drafts or other negotiable instruments with cash
- Nature of transactions inconsistent with what would be expected from declared business

Value of transactions

- Value just under the reporting threshold amount in an apparent attempt to avoid reporting
- Value inconsistent with the client's apparent financial standing

Examples of suspicious transactions for an intermediary

Identity of Client

- False identification documents
- Identification documents which could not be verified within reasonable time
- Non-face to face client

- Doubt over the real beneficiary of the account
- Accounts opened with names very close to other established business entities

Suspicious Background

- Suspicious background or links with known criminals

Multiple Accounts

- Large number of accounts having a common account holder, introducer or authorized signatory with no rationale
- Unexplained transfers between multiple accounts with no rationale

Activity in Accounts

- Unusual activity compared to past transactions
- Use of different accounts by client alternatively
- Sudden activity in dormant accounts
- Activity inconsistent with what would be expected from declared business
- Account used for circular trading

Nature of Transactions

- Unusual or unjustified complexity
- No economic rationale or bonafide purpose
- Source of funds are doubtful
- Appears to be case of insider trading
- Investment proceeds transferred to a third party
- Transactions reflect likely market manipulations
- Suspicious off market transactions

Value of Transactions

- Value just under the reporting threshold amount in an apparent attempt to avoid reporting
- Large sums being transferred from overseas for making payments

- Inconsistent with the clients apparent financial standing
- Inconsistency in the payment pattern by client
- Block deal which is not at market price or prices appear to be artificially inflated/deflated

Examples of suspicious transactions for an insurance company

- Customer insisting on anonymity, reluctance to provide identifying information, or providing minimal, seemingly fictitious information
- Cash based suspicious transactions for payment of premium and top ups. It should also consider multiple demand drafts each denominated for less than Rs.50,000
- Frequent free look cancellations by customers
- Assignments to unrelated parties without valid consideration
- Request for a purchase of policy in amount considered beyond his apparent need
- Policy from a place where he does not reside or is employed
- Frequent request for change in addresses
- Overpayment of premiums with a request for a refund of the amount overpaid

6) Counterfeit Currency Reports

The Prevention of Money-laundering Act, 2002, and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 require banking companies to report all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions.

7) Preparation of reports

The reporting entities are required to submit reports to FIU-IND which is compliant with the XML format specifications. Reporting entities which have necessary technical capabilities may generate XML (eXtensible Markup Language) reports directly from their systems. The reporting format guide – version 2.0 of 2011 provides reporting entities with the specifications of prescribed reports required to be submitted to the Financial Intelligence Unit – India (FIU-IND).

This document presents details of the XML schema and provides implementation guidance to the reporting entities in preparation and submission of reports.

The reporting formats specified in the reporting format guide are:

- Account based reporting format (ARF) for reporting of account based CTRs, STRs and NTRs
- Transactions based reporting format (TRF) for reporting of transaction based CTRs, STRs and NTRs
- CCR reporting format (CRF) for reporting of counterfeit currency reports (CCRs)

If the reporting entity has account-based relationship, they should use account based reporting format (ARF) for submitting CTR, STR and NTR. Transaction based reporting format (TRF) can be used for transactions without account based relationship with the customer. E.g. money transfer service, money exchange.

8) Submission of reports

With the implementation of Project FINnet (Financial Intelligence Network) by FIU-IND in 2010, the primary mode of submission of reports to FIU-IND will be through the FINnet Gateway Portal. The FINnet Gateway Portal - https://finnet.gov.in/ is designed as a comprehensive interface between the reporting entities and FIU-IND. The user guide for the FINnet Gateway Portal provides detailed documentation on using the portal.

Reporting Entities are expected to submit reports in electronic form. However if the reporting entity does not have the capability to generate report in electronic form, reports may be submitted in manual paper-based forms. Reporting Entities should use the FIU-IND provided PDF Form based utilities to capture data and print the report as per the specified format. The paper based report should be duly signed by the Principal Officer and posted to FIU-IND. However, Reporting Entities should make all reasonable efforts to send reports in electronic rather than the paper based format.

4.2.3. Due Diligence

One of the most important aspects of anti-money laundering measures with respect to financial transactions is client due diligence or customer due diligence. Client is the main cornerstone of any financial transaction. Every financial transaction revolves around a client. Hence the anti-money laundering measures with regard to a financial transaction will revolve only around a client. As mentioned earlier, client is a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who engaged in the transaction or activity, is acting. "Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes –

(i) opening of an account;

(ii) deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;

(iii) the use of a safety deposit box or any other form of safe deposit;

(iv) entering into any fiduciary relationship;

(v) any payment made or received in whole or in part of any contractual or other legal obligation;

(vi) any payment made in respect of playing games of chance for cash or kind including such activities associated with casino; and

(vii) establishing or creating a legal person or legal arrangement.

It is mandatory for every reporting entity, at the time of opening an account or executing any transaction with it, to verify the record of identity and current address or addresses including permanent address or addresses of the client, the nature of business of the client and his financial status. If it is not possible to verify the identity of the client at the time of opening an account or executing any transaction, the reporting entity should verify the identity of the client within a reasonable time after the account has been opened or the transaction has been executed. Every reporting entity should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the customer, his business and risk profile.

Client Due Diligence is dealt with under Rule 9 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005.

Documents required for verification are given hereunder –

Sl.No.	**Person**	**Verification**	**Documents (Certified copy)**
1.	**Individual**	Identity and address	Passport/ driving licence/ Permanent Account Number (PAN) Card/ Voter's Identity Card issued by the Election Commission of India/ identity card with applicant's Photograph issued by Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions/) letter issued by a gazetted officer, with a duly attested photograph of the person.
			One recent photograph
			Such other documents including the ones related to the nature of business and financial status of the client, as may be required by the banking company or the financial institution or the intermediary
2.	**Company**	Name, business, principal place of business of company and details of power of attorney holders	Certificate of incorporation

			Memorandum and Articles of Association
			A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf
			An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf
3.	**Partnership Firm**	Name, business, principal place of business of firm and details of power of attorney holders	Registration certificate
			Partnership deed
			An officially valid document in respect of the person holding an attorney to transact on its behalf
4.	**Trust**	Identity, address and details of power of attorney holders	Registration certificate
			Trust deed
			An officially valid document in respect of the person holding an attorney to transact on its behalf
5.	**Association of Persons (AOP) or Body of Individuals**	Identity, address and details of power of attorney holders	Resolution of the managing body of such an association or a body of individuals

	(BOI)		
			Power of attorney granted to (the authorized person) to transact on its behalf
			An officially valid document in respect of the person holding an attorney to transact on its behalf
			Such information as may be required by the banking company or the financial institution or the intermediary to collectively establish the legal existence of such an association or a body of individuals

Every reporting entity should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds.

When there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained client identification data, the reporting entity should review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be.

The reporting entity should apply client due diligence measures also to existing clients on the basis of materiality and risk, and conduct due diligence on such existing relationships at appropriate times or as may be specified by the regulator, taking into account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained.

Every reporting entity should formulate and implement a Client Due Diligence Programme. The Client Due Diligence Programme should include policies, controls and procedures, approved by the senior management, to enable the reporting entity to manage and mitigate the risk that have been identified either by the reporting entity or through national risk assessment.

5. HOW TO ENSURE EFFECTIVE KYC IN FINANCIAL TRANSACTIONS?

Without understanding the regulations and the anti-money laundering regulations and financial sanctions regimes, risk assessments undertaken by financial institutions are likely to be inaccurate and consequently, systems and controls put in place to prevent non-compliance might not be effective or efficient. Financial institutions have to be increasingly proactive and vigilant in their daily operations and transactions to deal with the conflicting and overlapping sanctions regimes in addition to continuous efforts to comply with anti-money laundering regulations. Regular risk assessment reviews are a priority for financial institutions that are striving to maintain operationally effective systems.

5.1. What is Know Your Customer (KYC)?

KYC is an acronym for "Know your Customer", a term used for customer identification process. It involves making reasonable efforts to determine true identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business, etc which in turn helps the financial institutions to manage their risks prudently.

KYC has two components - Identity and Address. While identity remains the same, the address may change and hence the banks are required to periodically update their records.

The objective of KYC guidelines is to prevent financial institutions from being used, intentionally or unintentionally, by criminal elements for money laundering activities. Related procedures also enable financial institutions especially banks to know or understand their customers, and their financial dealings better. This helps them manage their risks prudently. Banks usually frame their KYC policies incorporating the following four key elements:

- Customer Acceptance Policy;
- Customer Identification Procedures;
- Monitoring of Transactions; and

- Risk management.

KYC controls typically include the following;

- Collection and analysis of basic identity information (referred to as "Customer Identification Program")
- Name matching against lists of known parties (such as "politically exposed person" or PEP)
- Determination of the customer's risk in terms of propensity to commit money laundering, terrorist finance, or identity theft
- Creation of an expectation of a customer's transactional behavior
- Monitoring of a customer's transactions against their expected behaviour and recorded profile as well as that of the customer's peers.

5.2. Origin of concept of KYC

The concept of KYC is at once ancient and revolutionary. The nineteenth century shopkeeper built long-term relationships with his customers. The storeowner knew customers personally, could greet them, anticipate their needs, and win their continued business. In today's markets dominated by large corporations, relationships cannot be built around a customer contacting the same company employee every time. Instead technology allows firms of all sizes to collect and store information about customers at every opportunity, and make it available to company employees in order to personalize the service whenever they have contact with customers. In essence, today's company knows its customers through its database.[1]

The focus on preventing money laundering took a new turn with September 11 terrorist attacks in U.S. The events highlighted the need to combat terrorist financing as an integral part of anti-money laundering (AML) processes. Until that time, financial institutions and intelligence agencies essentially focused on movement of funds related to drug trade and large scale financial

[1] Michael E. Staten & Fred H. Cate, The Impact of Opt-In Privacy Rules On Retail Credit Markets: A Case Study of MBNA, 52 Duke L.J. 745 (2003)

fraud. It is believed funds necessary to enable execution of the 9/11 plot were primarily moved through the international financial system and withdrawn in the US through formal banking channels (encashment of travelers cheques, cash withdrawal through ATMs and credit cards). The entire plot is expected to have been executed with a budget of $400,000 - $500,000. Further the hijackers also returned about $26,000 to a facilitator in the middle-east just days prior to the attack. The US government became very strict after September 11 terrorist attacks and all regulations for KYC were finalized before 2002. The US has made changes in its major legislations — Bank Secrecy Act, USA Patriot Act, etc. to make KYC norms really effective for the banking sector.

Taking a leaf out of the US book, the Reserve Bank of India too directed all banks to implement KYC guidelines for all new accounts in the second half of 2002. For existing accounts, imposing KYC norms was a little difficult, so the RBI issued guidelines for it at the end of 2004. Thereafter RBI has been updating the KYC norms for banks, co-operative banks and NBFCs to be followed.

The idea was later adopted by IRDA for issuing out insurance policies to investors and later by SEBI for opening brokerage accounts. Eventually, all financial transactions were covered under KYC norms.

Although each authority like RBI, SEBI, IRDA etc. have issued separate KYC norms, all the guidelines are substantially identical. Only difference is that flexibility is promoted in the norms to accommodate the different types of financial institutions under their supervision.

Recently the Reserve Bank of India imposed a fine of Rs.49.5 crore on 22 banks for violation of KYC norms, following investigations into allegations of money laundering leveled against them. Although the investigations did not bring out any instance of money laundering but resulted in the largest collective penalty on Indian banks for violation of 'know your customer' norms that are aimed at preventing money laundering.

The violations for which the penalties have been imposed include omission in reporting cash transaction limits, sale of gold coins for cash beyond Rs 50,000, non-adherence to instructions on monitoring transactions, failing to stick to the limit for remittance or repatriation of funds abroad and importing of gold on consignment basis.

5.3. Purpose of KYC Guidelines

- It will deter criminals posing as legitimate customers who would use financial institutions as tools to launder proceeds from their illicit activities.
- Strict adherence to KYC guidelines may reveal the illicit nature of a customer's business.
- The information obtained from a customer will be transferred onto a database that will indicate when transactions are inconsistent with a customer's normal business transactions.

The basic object of KYC guidelines were designed to prevent entry of illicit funds into the system and to keep banks from becoming unwitting participants in money launderings schemes. Financial institutions with sound KYC guidelines in place will have the ability to prevent the opening of fictitious accounts and will provide the financial institutions with a customer profile that will enable it to predict, with relative certainty, the types of transactions in which the customer is likely to engage.

5.4. Know Your Customer (KYC) Norms/Obligations of Banks

Detailed guidelines on KYC norms, anti-money laundering standards and combating of financing of terrorism have been issued by the Reserve Bank of India. All the instructions/guidelines have been consolidated under the Master Circular DBOD. AML. BC. No. 24/14.01.001/2013-14 dated July 1, 2013. The instructions, contained in the master circular, are applicable to All India Financial Institutions, all scheduled commercial banks (excluding RRBs) and Local Area Banks. The guidelines will apply to the branches and majority owned subsidiaries located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of Reserve Bank. In case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of banks are required to adopt the more stringent regulation of the two.

It has been issued under Section 35A of the Banking Regulation Act, 1949 and Rule 7 of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. Hence, any contravention thereof or non-compliance will attract penalties under the respective Acts.

The banks have to ensure that a proper policy framework on 'Know your customer' and anti-money laundering measures is formulated with the approval of their Board and put in place.
For the purpose of KYC policy, a 'Customer' is defined as:

(*a*) a person or entity that maintains an account and/or has a business relationship with the bank;

(*b*) one on whose behalf the account is maintained (i.e. the beneficial owner);

(*c*) beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and

(*d*) Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

To prevent the possible misuse of banking activities for anti-national or illegal activities, the RBI has given various directives to banks:

1. Strengthen the banks' 'Internal Control System' by allocating duties and responsibilities to their staff and periodically monitor them.
2. Before giving any finance at branch level, make sure that the person has no links with notified terrorist entities and report any such 'suspect' accounts to the government.
3. Regular 'Internal Audit' by internal and concurrent auditors to check if the KYC guidelines are being properly adhered to by the banks.

Every bank should frame their KYC policies incorporating the following four key elements:

i. Customer Acceptance Policy
ii. Customer Identification Procedure
iii. Monitoring of transactions

iv. Risk management

(1) Customer Acceptance Policy

Every bank should develop a clear Customer Acceptance policy laying down explicit criteria for Acceptance of customers. The Customer Acceptance policy must ensure that explicit guidelines are in place on the following aspects of customer relationship in the bank:-

1. No account is opened in anonymous or fictitious benami name.
2. Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorization of customers into low, medium and high risk. Customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs) may, if considered necessary, be categorized even higher.
3. Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and instructions/guidelines issued by Reserve Bank from time to time.
4. Not to open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures, i.e., bank is unable to verify the identity and /or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of the data/information furnished to the bank. It is, however, necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision by a bank to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.
5. Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity.

6. Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organisations etc.

Banks should prepare a profile for each new customer based on risk categorization. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. While preparing customer profile banks should take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein should not be divulged for cross selling or any other purposes.

For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorized as low risk. Examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Customers that are likely to pose a higher than average risk to the bank should be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc. Banks should apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. In view of the risks involved in cash intensive businesses, accounts of bullion dealers (including sub-dealers) & jewelers should also be categorized by banks as 'high risk' requiring enhanced due diligence. Other examples of customers requiring higher due diligence include (a) nonresident customers; (b) high net worth individuals; (c) trusts, charities, NGOs and organizations receiving donations; (d) companies having close family shareholding or beneficial ownership; (e) firms with 'sleeping partners'; (f) politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner; (g) non-face to face customers and

(h) those with dubious reputation as per public information available etc. However, only NPOs/NGOs promoted by United Nations or its agencies may be classified as low risk customers.

In addition to the above, banks/financial institutions should take steps to identify and assess their Money Laundering/Terrorist Financing risk for customers, countries and geographical areas as also for products/ services/ transactions/delivery channels, Banks/FIs should have policies, controls and procedures, duly approved by their boards, in place to effectively manage and mitigate their risk adopting a risk-based approach. As a corollary, banks would be required to adopt enhanced measures for products, services and customers with a medium or high risk rating.

But every bank needs to ensure that the adoption of customer acceptance policy and its implementation does not become too restrictive and must not result in denial of banking services to general public especially to those who are financially or socially disadvantaged.

(2) Customer Identification Procedure (CIP)

Customer Identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information.

The policy approved by the Board of banks should clearly spell out the Customer Identification Procedure to be carried out at different stages i.e. while establishing a banking relationship; carrying out a financial transaction or when the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data. Banks need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship. Being satisfied means that the bank must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk-based approach is considered necessary to avoid disproportionate cost to banks and a burdensome regime for the customers.

For customers that are natural persons, the banks should obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph.

For customers that are legal persons or entities, the bank should (*i*) verify the legal status of the legal person/entity through proper and relevant documents; (*ii*) verify that any person purporting to act on behalf of the legal person/entity is so authorised and identify and verify the identity of that person; (*iii*) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

The increasing complexity and volume of financial transactions necessitate that customers do not have multiple identities within a bank, across the banking system and across the financial system. This can be achieved by introducing a unique identification code for each customer. The Unique Customer Identification Code (UCIC) will help banks to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers. It would also smoothen banking operations for the customers. While some banks already use UCIC for their customers by providing them a relationship number, etc., other banks have not adopted this practice. Banks have been advised to initiate steps for allotting UCIC to all their customers while entering into any new relationships for individual customers to begin with. Existing individual customers were required to be allotted UCIC by end-May 2013. However, in view of difficulties expressed by some banks in implementing UCIC for their customers, for various reasons, and keeping in view the constraints, the time for completing the process of allotting UCIC to existing customers has been extended up to March 31, 2014.

Whenever there is suspicion of money laundering or terrorist financing or when other factors give rise to a belief that the customer does not, in fact, pose a low risk, banks should carry out full scale customer due diligence (CDD) before opening an account. When there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained customer identification data, banks should review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship.

Banks should introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. The periodicity of such updation should not be less than once in five years in case of low risk category customers and not less than once in two years in case of high and medium risk categories. Such verification should be done

irrespective of whether the account has been transferred from one branch to another and banks are required to also maintain records of transactions.

Customer Identification Requirements

i. In case of transactions carried out by a **non-account based customer**, that is a walk-in customer, where the amount of transaction is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified. However, if a bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000/- the bank should verify the identity and address of the customer and also consider filing a suspicious transaction report (STR) to FIU-IND. Banks and financial institutions are required to verify the identity of the customers for all international money transfer operations.

ii. In case of **salaried employees**, with a view to containing the risk of fraud, banks should rely on certificate/letter of identity and/or address issued only from corporate and other entities of repute and should be aware of the competent authority designated by the concerned employer to issue such certificate/letter. Further, in addition to the certificate/letter issued by the employer, banks should insist on at least one of the officially valid documents as provided in the Prevention of Money Laundering Rules (viz. passport, driving licence, PAN Card, Voter's Identity card, etc.) or utility bills for KYC purposes for opening bank accounts of salaried employees of corporate and other entities.

iii. Sometimes **trust/nominee or fiduciary accounts** can be used to circumvent the customer identification procedures. Banks should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, banks should insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, banks should take reasonable precautions to verify the identity of the trustees and

the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

iv. Banks should be vigilant against **business entities** being used by individuals as a 'front' for maintaining accounts with banks. Banks should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

v. When the bank has knowledge or reason to believe that the **client account opened by a professional intermediary** is on behalf of a single client, that client must be identified. Banks may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the bank, the bank should still look through to the beneficial owners. Where the banks rely on the 'customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements.

vi. Banks should not allow opening and/or holding of an account on behalf of a client/s by **professional intermediaries, like Lawyers and Chartered Accountants**, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits bank's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, should not be allowed to open an account on behalf of a client.

vii. With the introduction of telephone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. In the case of **non-face-to-face customers**, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented should be insisted upon and, if necessary, additional documents may be called for. In such cases, banks may also require the first payment to be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

viii. Apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, banks should call for and verify the following documents before opening of accounts in the name of a **proprietary concern** –

a. Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/licence issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST/VAT certificate, certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities, Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, registration/licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/Department. Banks may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT, the complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities and utility bills such as electricity, water, and landline telephone bills in the name of

the proprietary concern as required documents for opening of bank accounts of proprietary concerns. Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.

Politically Exposed Persons (PEPs) resident outside India

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Banks should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Banks should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for a PEP should be taken at a senior level which should be clearly spelt out in Customer Acceptance Policy. Banks should also subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs. In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, banks should obtain senior management approval to continue the business relationship and subject the account to the Customer due diligence (CDD) measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis. This will also be applicable to accounts where a PEP is the ultimate beneficial owner. Further, banks should have appropriate ongoing risk management procedures for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner.

(3) Monitoring of Transactions

Ongoing monitoring of transactions is an essential element of effective KYC procedures. Banks should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being washed through the account. High-risk accounts have to be subjected to intensified monitoring. Every

bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. High risk associated with accounts of bullion dealers (including sub-dealers) & jewelers should be taken into account by banks to identify suspicious transactions for filing Suspicious Transaction Reports (STRs) to Financial Intelligence Unit- India (FIU-IND). There should be a periodical review of risk categorization of accounts that should be carried out at a periodicity of not less than once in six months.

Accounts of Multi-level Marketing (MLM) Companies are misused for defrauding public by luring them into depositing their money with the MLM company by promising a high return. Such depositors are assured of high returns and issued post-dated cheques for interest and repayment of principal. So long as money keeps coming into the MLM Company's account from new depositors, the cheques are honoured but once the chain breaks, all such post-dated instruments are dishonoured. This results in fraud on the public and is a reputational risk for banks concerned. Further, banks should closely monitor the transactions in accounts of marketing firms. In cases where a large number of cheque books are sought by the company, there are multiple small deposits (generally in cash) across the country in one bank account and where a large number of cheques are issued bearing similar amounts/dates, the bank should carefully analyse such data and in case they find such unusual operations in accounts, the matter should be immediately reported to Reserve Bank and other appropriate authorities such as Financial Intelligence Unit India (FIU-Ind) under Department of Revenue, Ministry of Finance.

Banks should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds

The risk categorization of customers as also compilation and periodic updation of customer profiles and monitoring and closure of alerts in accounts by banks are extremely important for effective implementation of KYC/AML/CFT measures.

Where the bank is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the bank should consider closing the account or terminating the banking/business relationship after issuing due notice to the customer

explaining the reasons for taking such a decision. Such decisions need to be taken at a reasonably senior level.

(4) Risk Management

The Board of directors of every bank should ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It should cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility should be explicitly allocated within the bank for ensuring that the bank's policies and procedures are implemented effectively. Banks should, in consultation with their boards, devise procedures for creating risk profiles of their existing and new customers, assess risk in dealing with various countries, geographical areas and also the risk of various products, services, transactions, delivery channels, etc.

Banks internal audit and compliance function have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Banks should ensure that their audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Concurrent/Internal Auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard should be put up before the Audit Committee of the Board on quarterly intervals.

Banks should pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Many banks are engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Banks are required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Further, marketing of credit cards is generally done through the services of agents. Banks should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that agents are also subjected to KYC measures.

Combating Financing of Terrorism

Banks are advised to develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to FIU-Ind on priority.

As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank circulates these to all banks and financial institutions. Banks/Financial Institutions should ensure to update the lists of individuals and entities as circulated by Reserve Bank.

Banks are advised that before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the lists. Further, banks should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to RBI and FIU-IND.

Correspondent Banking

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc. Banks should gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Information on the other bank's management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the correspondent's/respondent's country may be of special relevance. Similarly, banks should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. While it is desirable that such relationships should be established only with the approval of the Board, in case the Boards of some banks wish to delegate the power to an administrative authority, they may

delegate the power to a committee headed by the Chairman/CEO of the bank while laying down clear parameters for approving such relationships. Proposals approved by the Committee should invariably be put up to the Board at its next meeting for post facto approval. The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented. In the case of payable-through-accounts, the correspondent bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them. The correspondent bank should also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

Correspondent relationship with a "Shell Bank"

Banks should refuse to enter into a correspondent relationship with a **"**shell bank**"** (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group). Shell banks are not permitted to operate in India. Banks should not enter into relationship with shell banks and before establishing correspondent relationship with any foreign institution, banks should take appropriate measures to satisfy themselves that the foreign respondent institution does not permit its accounts to be used by shell banks. Banks should be extremely cautious while continuing relationships with correspondent banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing. Banks should ensure that their respondent banks have anti money laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

Wire Transfer

Banks use wire transfers as an expeditious method for transferring funds between bank accounts. Wire transfers include transactions occurring within the national boundaries of a country or from one country to another. As wire transfers do not involve actual movement of currency, they are considered as a rapid and secure method for transferring value from one location to another.

- Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of

money available to a beneficiary person at a bank. The originator and the beneficiary may be the same person.

- Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institutions are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.
- Domestic wire transfer means any wire transfer where the originator and receiver are located in the same country. It may also include a chain of wire transfers that takes place entirely within the borders of a single country even though the system used to effect the wire transfer may be located in another country.
- The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the bank to perform the wire transfer.

Wire transfer is an instantaneous and most preferred route for transfer of funds **across** the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analysing suspicious or unusual activity and disseminating it as necessary. The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits. Hence, banks must ensure that all wire transfers are accompanied by the following information:

Cross-border wire transfers

All cross-border wire transfers should be accompanied by accurate and meaningful originator information. Information accompanying cross-border wire transfers should contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be

included. Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as mentioned above.

Domestic wire transfers

Information accompanying all domestic wire transfers of Rs.50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means. If a bank has reason to believe that a customer is intentionally structuring wire transfer to below Rs. 50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the bank must insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be made to FIU-IND. It will be applicable in case where a credit or debit card is used to effect money transfer.

Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions would be exempted from the above requirements.

Principal Officer

Every bank should appoint a senior management officer to be designated as Principal Officer. The Principal Officer should be able to act independently and report directly to the senior management or to the Board of Directors. He should be located at the head/corporate office of the bank and be responsible for monitoring and reporting all transactions and sharing of information as required under the law. He should maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism. The role and responsibilities of the Principal Officer should include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made thereunder, as amended form time to time. The Principal Officer will also be responsible for timely submission of Cash Transaction Reports, Suspicious Transactions Reports and reporting of counterfeit notes and all transactions

involving receipts by non-profit organisations of value more than Rupees Ten Lakh or its equivalent in foreign currency to FIU-IND. With a view to enabling the Principal Officer to discharge his responsibilities effectively, the Principal Officer and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records and other relevant information.

Customer Education/Employee's Training/Employee's Hiring

Banks should prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the KYC programme. The front desk staff should be specially trained to handle such situations while dealing with customers. Banks must have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements should have different focuses for frontline staff, compliance staff and staff dealing with new customers. Adequate screening mechanism should be put in place by banks as an integral part of their recruitment/hiring process of personnel.

5.5. KYC Norms and AML standards – Guidance Notes for Banks

The Indian Banks' Association has issued "Know Your Customer (KYC) Standards and Anti-Money Laundering (AML) Measures - IBA Guidance Notes for Banks. This gives a broad outline of policy frame work based on international practices to serve as a reference guide to banks in complying with the provisions of the Reserve Bank of India guidelines on "Know Your Customer Guidelines and Anti-Money Laundering Standards" and also to meet the obligations of banks under the Prevention of Money Laundering Act (PMLA) 2002. The IBA Guidance Notes are useful in ensuring uniformity of approach among the banks in implementing the KYC Norms and AML Standards. It facilitates banks to align their operations with good international industry practices in AML / CFT procedures through an appropriate risk based approach and provides a framework for banks to design and implement the systems and controls necessary to mitigate the risks of the bank being used in connection with money laundering and terrorist financing.

The purpose of this Guidance Notes is to:

- Create awareness to the legal and regulatory frame work for AML/CFT requirements and systems across the banking sector
- Interpret the obligations under the PMLA and other relevant regulations and how they may be implemented in practice
- Help banks to align their operations with good international industry practice in AML/CFT procedures through a proportionate risk based approach
- Provide a framework for banks to design and implement the systems and controls necessary to mitigate the risks of the bank being used in connection with money laundering and terrorist financing.

Although these Guidance Notes are designed primarily to cover the activities of banks, the contents are generally applicable to other financial institutions and intermediaries covered under the PMLA and are required to adopt KYC Standards.

Guidance Notes issued by IBA are voluntary and recommendatory in nature. Failure to comply with these Guidance Notes does not mean that a Bank has automatically breached the Rules under PMLA or any of the Guidelines issued by RBI. They do, however, provide an indication of what the supervisors/ regulators may take into account as being expected of banks. When tailored by a bank to its own risk management architecture and business processes, these Guidelines provide a safety net in respect of Rules and Regulations pertaining to AML.

The following are covered under the Guidance notes –

- Overview and Regulatory Frame Work
- Internal Controls and Structure in Banks
- Customer Risk Categorization (CRC)
- Know Your Customer (KYC)
- Reporting Obligation under PMLA Act
- Transaction Monitoring
- Name Screening Process
- Wire Transfers

- Staff and Customer Awareness
- Preservation of Records

5.6. Know Your Customer (KYC) Norms/Obligations of NBFCs

Detailed guidelines on KYC norms, anti-money laundering standards and combating of financing of terrorism applicable for non-banking financial companies (NBFCs) have been issued by the Reserve Bank of India. All the instructions/guidelines have been consolidated under the Master Circular DNBS (PD) CC No.339 /03.10.42/ 2013-14 dated July 1, 2013.

The instructions, contained in the master circular, are applicable to all NBFCs including brokers/agents etc. collecting public deposits on behalf of NBFCs. The KYC/AML guidelines issued by Reserve Bank of India will also apply to their branches and majority owned subsidiaries located outside India, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. In case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of NBFCs are required to adopt the more stringent regulation of the two.

It has been issued under Sections 45K and 45L of the RBI Act, 1934 and Rule 7 of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. Hence, any contravention thereof or non-compliance will attract penalties under the respective Acts.

The NBFCs have to ensure that a proper policy framework on 'Know your customer' and anti-money laundering measures is formulated with the approval of their Board and put in place.

For the purpose of KYC policy, a 'Customer' is defined as:

(*a*) a person or entity that maintains an account and/or has a business relationship with the bank;

(*b*) one on whose behalf the account is maintained (i.e. the beneficial owner);

(*c*) beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and

(*d*) Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

Obligations to be followed by NBFCs

1) Adherence to KYC guidelines

Adherence to KYC guidelines by NBFC and persons authorized by NBFCs including brokers/agents etc. is compulsory.

In case of RNBCs (residuary non-banking companies), for the existing customers, initially, KYC guidelines should be complied in respect of large customers whose aggregate deposit exceeds Rs.1 lakh. For the remaining existing accounts, the companies should ensure that the details of the customers are updated at the time of renewal of the deposit. This should, however, not result in unnecessary harassment of customers.

2) Due diligence of persons authorized by NBFCs including brokers/agents etc.

NBFCs should put in place a process of due diligence in respect of persons authorised by NBFCs including brokers/agents etc. collecting deposits on behalf of the company through a uniform policy for appointment and detailed verification. The companies should have systems in place to ensure that the books of accounts of persons authorized by NBFCs including brokers/agents etc, so far as they relate to brokerage functions of the company, are available for audit and inspection whenever required.

3) Customer service in terms of identifiable contact with persons authorised by NBFCs including brokers/agents etc.

All deposit receipts should bear the name and Registered Office address of the NBFC and must invariably indicate the name of the persons authorised by NBFCs including brokers/agents etc. and their addresses who mobilised the deposit and the link office with the telephone number of such officer and/or persons authorised by NBFCs including brokers/ agents etc. in order that there is a clear indication of the identifiable contact with the field persons and matters such as unclaimed/lapsed deposits, discontinued deposits, interest payments and other customer

grievances are appropriately addressed. The companies can also evolve suitable review procedures to identify persons authorised by NBFCs including brokers/agents etc. in whose cases the incidence of discontinued deposits is high for taking suitable action.

NBFCs are required to put in place a system of periodical review of risk categorisation of accounts and the need for applying enhanced due diligence measures in case of higher risk perception on a customer. Review of risk categorisation of customers should be carried out at a periodicity of not less than once in six months. NBFCs should also introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. The periodicity of such updation should not be less than once in five years in case of low risk category customers and not less than once in two years in case of high and medium risk categories.

4) Letter issued by Unique Identification Authority of India (UIDAI)

Letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number is recognized as an officially valid document. While opening accounts based on Aadhaar, NBFCs must satisfy themselves about the current address of the customer by obtaining required proof of the same.

NBFCs have been advised by RBI to initiate steps for allotting Unique Customer Identification Code (UCIC) to all their customers while entering into any new relationships. Similarly, existing individual customers should also be allotted UCIC.

5) Accounts of Politically Exposed Persons (PEPs)

NBFCs should have appropriate ongoing risk management procedures for identifying and applying enhanced CDD (customer due diligence) to PEPs (Politically exposed person), customers who are close relatives of PEPs, and accounts of which PEP is the ultimate beneficial owner. In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, NBFCs (including RNBCS) should obtain senior management approval to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis.

6) Client accounts opened by professional intermediaries

If the NBFC has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. NBFCs may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. NBFCs also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the NBFCs and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the NBFC, the NBFC should still look through to the beneficial owners. If a NBFC decides to accept an account in terms of the Customer Acceptance Policy, NBFC should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are. It is not possible for professional intermediaries like Lawyers and Chartered Accountants, etc. who are bound by any client confidentiality that prohibits disclosure of the client details, to hold an account on behalf of their clients.

NBFCs should not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality.

7) Internal guidelines

Internal guidelines for customer identification procedure of legal entities may be framed by NBFCs based on their experience of dealing with such entities, normal lenders prudence and the legal requirements as per established practices.

8) Principal Officer

NBFCs (including RNBCs) should appoint a senior management officer to be designated as Principal Officer for overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made there under. The Principal Officer and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records and other relevant information. NBFCs (including RNBCs)

should ensure that the Principal Officer is able to act independently and report directly to the senior management or to the Board of Directors.

9) Suspicion of money laundering/terrorist financing

Whenever there is suspicion of money laundering or terrorist financing or when other factors give rise to a belief that the customer does not, in fact, pose a low risk, NBFCs should carry out full scale customer due diligence (CDD) before opening an account.

5.7. Anti Money Laundering (AML) Standards/ Obligations of Securities Market Intermediaries

According to Sec.2(1)(n) of the Prevention of Money Laundering Act, 2002, Intermediary means-

(i) a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser or any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992; or

(*ii*)an association recognised or registered under the Forward Contracts (Regulation) Act, 1952 or any member of such association; or

(*iii*)intermediary registered by the Pension Fund Regulatory and Development Authority; or

(*iv*)a recognised stock exchange referred to in clause (*f*) of section 2 of the Securities Contracts (Regulation) Act, 1956

SEBI has issued necessary directives vide circulars, from time to time, covering issues related to Know Your Client (KYC) norms, Anti- Money Laundering (AML), Client Due Diligence (CDD) and Combating Financing of Terrorism (CFT). The Master Circular dated 31-12-2010 provides a detailed account of the procedures and obligations to be followed by all registered intermediaries to ensure compliance with AML/CFT directives.

The senior management of a registered intermediary should be fully committed to establishing appropriate policies and procedures for the prevention of Money Laundering and Terrorist Financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements.

Policies and procedures to combat Money Laundering should cover:

(*a*) Communication of group policies relating to prevention of Money Laundering and Terrorist Financing to all management and relevant staff that handle account information, securities transactions, money and client records etc. whether in branches, departments or subsidiaries;

(*b*) Client acceptance policy and client due diligence measures, including requirements for proper identification;

(*c*) Maintenance of records;

(*d*) Compliance with relevant statutory and regulatory requirements;

(*e*) Co-operation with the relevant law enforcement authorities, including the timely disclosure of information; and

(*f*) Role of internal audit or compliance function to ensure compliance with the policies, procedures, and controls relating to the prevention of Money Laundering and Terrorist Financing, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff, of their responsibilities in this regard. The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and other such factors.

Each registered intermediary should adopt written procedures to implement the anti money laundering provisions as envisaged under the Act. Such procedures should include inter alia, the following three specific parameters which are related to the overall 'Client Due Diligence Process':

(*a*) Policy for acceptance of clients

(*b*) Procedure for identifying the clients

(*c*) Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR).

The KYC policy should clearly spell out the client identification procedure to be carried out at different stages i.e. while establishing the intermediary – client relationship, while carrying out transactions for the client or when the intermediary has doubts regarding the veracity or the adequacy of previously obtained client identification data.

Intermediaries should take appropriate steps to evolve an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities.

5.8. SEBI {KYC (Know Your Client) Registration Agency} Regulations, 2011

Various SEBI Circulars issued since the year 1993 read with the Prevention of Money Laundering Act and Rules as amended from time to time, have prescribed mandatory procedures for intermediaries to undertake the activity of Customer Due Diligence (CDD) or Know Your Client (KYC) with regard to account opening and ongoing transaction monitoring. SEBI Master Circular on Anti-Money Laundering (dated 31/12/2010) while invoking the PML Rules mandates detailed activities upon all intermediaries regulated by SEBI while accepting clients. Many SEBI's Circulars on KYC pre-date the PML Rules and are directed separately to each class or type of intermediary in the securities market. Earlier, KYC was done by each SEBI regulated intermediary viz. Broker, Depository Participant (DP), Mutual Fund, Portfolio Manager etc. As a result, from the perspective of a client, if a client were to open an account with different types of intermediaries or more than one intermediary of the same type, as would be expected of a client, it would have to undergo the KYC process with each intermediary. This resulted in duplication of work, wastage of recordkeeping space and was a burden on the intermediaries and even more so to the client seeking to make investments. Over time variations have emerged in prescribed procedures for undertaking KYC by different classes of

intermediaries within the securities market. This pointed to gaps in achieving a common KYC standard in the securities market. For instance directions given by SEBI, the Exchanges and Depositories to brokers and DPs respectively, mandate a more rigorous performance of KYC by these intermediaries as compared to directions to Portfolio Managers. This worked as a disincentive for ease of entry of potential clients in the securities market.

An internal committee was constituted to examine the current practices and suggest changes with a view to address the identified problems or gaps. Some of the proposals suggested by the Committee were –

- initial KYC should be undertaken only once and the client should not be made to repeatedly fill up the same form and submit documents when he wishes to open an account with another intermediary registered with SEBI
- uniform format to be used by all intermediaries for this activity
- KYC could be undertaken by third parties
- one or more SEBI regulated KYC Registration Agency (KRA) will undertake KYC at the stage of account opening for all clients in the securities market through the Points of Service (PoS). Only SEBI regulated intermediaries will be permitted to serve as PoS. The KRAs would also serve as a repository of KYC data or identification documents
- execution of a single and uniform KYC procedure across the securities market
- periodical update by KRA
- centralized storage and dissemination of data gathered due to the combined action of several intermediaries

Pursuant to this, the SEBI issued the SEBI {KYC (Know Your Client) Registration Agency (KRA)}, Regulations of 2011.

KYC Registration Agency (KRAs) registered with SEBI are –

i. CDSL Ventures Limited (CVL) - www.cvlindia.com
ii. NSDL Database Management Limited (NDML) - www.ndml.in
iii. DotEx International Limited (DotEx) - www.nseindia.com/supra_global/content/dotex/about_dotex.htm

iv. CAMS Investor Services Private Limited. - www.camskra.com

v. Karvy Data Management Services Limited - http://www.karvykra.com

Functions and obligations of KRA

KRA provides for centralization of the KYC records in the securities market. The client who is desirous of opening an account/trade/deal with the SEBI registered Intermediary shall submit the KYC details through the KYC Registration form and supporting documents. The Intermediary shall perform the initial KYC and upload the details on the system of the KYC Registration Agency (KRA). This KYC information can be accessed by all the SEBI Registered Intermediaries while dealing with the same client. As a result, once the client has done KYC with a SEBI registered intermediary, he need not undergo the same process again with another intermediary.

Regulation 15 of SEBI KRA Regulations 2011 defines the roles and obligations of KRA.

- KRA shall be responsible for storing, safeguarding and retrieving the KYC documents that are being submitted by various SEBI registered intermediaries.
- KRA shall retain the original KYC documents of the client, in both physical and electronic form for the period specified, as well as ensuring that retrieval of KYC information is facilitated within stipulated time period.
- Any information updated about a client shall be disseminated by KRA to all intermediaries that avail of the services of the KRA in respect of that client.
- KRA(s) shall have electronic connectivity and with other KRA(s) in order to establish inter-operability among KRAs.
- KRA shall send a letter to each client after receipt of the KYC documents from the intermediary, confirming the client's details thereof.
- KRA shall take adequate steps for redressal of the grievances of the clients within one month of the date of receipt of the complaint.

Role of intermediaries in KRA

Regulation 16 of SEBI KRA Regulations 2011 defines the roles and obligations of Intermediaries.

- The intermediary shall perform the initial KYC/due diligence of the client, shall upload the KYC information / documents on the system of the KRA and send the original KYC documents to KRA within the prescribed time.
- When the client approaches another intermediary subsequently, it will be optional for the intermediary to verify and download the client's details from the system of KRA or to take fresh KYC as per existing system.
- However, upon receipt of information on change in KYC details and status of the clients by the intermediary or when it comes to the knowledge of the intermediary, at any stage, the intermediary shall be responsible for uploading the updated information on the system of KRA and for sending the physical documents to KRA, wherever necessary.
- An intermediary shall not use the KYC data of a client obtained from the KRA for purposes other than it is meant for; nor shall it make any commercial gain by sharing the same with any third party including its affiliates or associates.
- The intermediary shall have the ultimate responsibility for the KYC of its clients, by undertaking enhanced KYC measures commensurate with the risk profile of its clients.

5.8.1. SEBI Guidelines in pursuance of the SEBI KYC Registration Agency (KRA) Regulations, 2011 and for In-Person Verification (IPV)

1) Guidelines for Intermediaries:

I. After doing the initial KYC of the new clients, the intermediary should forthwith upload the KYC information on the system of the KRA and send the KYC documents i.e. KYC application form and supporting documents of the clients to the KRA within 10 working days from the date of execution of documents by the client and maintain the proof of dispatch.

II. In case a client's KYC documents sent by the intermediary to KRA are not complete, the KRA should inform the same to the intermediary who shall forward the required information / documents promptly to KRA.

III. For existing clients, the KYC data may be uploaded by the intermediary provided they are in conformity with details sought in the uniform KYC form prescribed vide SEBI circular no. MIRSD/SE/Cir-21/2011 dated October 05, 2011. While uploading these clients' data the intermediary should ensure that there is no duplication of data in the KRA system.

IV. The intermediary should carry out KYC when the client chooses to trade/ invest / deal through it.

V. The intermediaries should maintain electronic records of KYCs of clients and keeping physical records would not be necessary.

VI. The intermediary should promptly provide KYC related information to KRA, as and when required.

VII. The intermediary should have adequate internal controls to ensure the security / authenticity of data uploaded by it.

2) Guidelines for KRAs:

I. KRA system should provide KYC information in data and image form to the intermediary.

II. KRA should send a letter to the client within 10 working days of the receipt of the initial/updated KYC documents from intermediary, confirming the details thereof and maintain the proof of dispatch.

III. KRA(s) should develop systems, in co-ordination with each other, to prevent duplication of entry of KYC details of a client and to ensure uniformity in formats of uploading / modification / downloading of KYC data by the intermediary.

IV. KRA should maintain an audit trail of the upload / modifications / downloads made in the KYC data, by the intermediary in its system.

V. KRA should ensure that a comprehensive audit of its systems, controls, procedures, safeguards and security of information and documents is carried out annually by an independent auditor. The Audit Report along with the steps taken to rectify the deficiencies, if any, shall be placed before its Board of Directors. Thereafter, the KRA should send the Action Taken Report to SEBI within 3 months.

VI. KRA systems should clearly indicate the status of clients falling under PAN exempt categories viz. investors residing in the state of Sikkim, UN entities / multilateral agencies exempt from paying taxes / filing tax returns in India.

VII. A client can start trading / investing/ dealing with the intermediary and its group / subsidiary / holding company as soon as the initial KYC is done and other necessary information is obtained while the remaining process of KRA is in progress.

3. In-Person Verification (IPV):

I. The intermediary should ensure that the details like name of the person doing IPV, his designation, organization with his signatures and date are recorded on the KYC form at the time of IPV.

II. The IPV carried out by one SEBI registered intermediary can be relied upon by another intermediary.

III. In case of Stock brokers, their sub-brokers or Authorised Persons (appointed by the stock brokers after getting approval from the concerned Stock Exchanges in terms of SEBI Circular No. MIRSD/DR-1/Cir-16/09 dated November 06, 2009) can perform the IPV.

IV. In case of Mutual Funds, their Asset Management Companies (AMCs) and the distributors who comply with the certification process of National Institute of Securities Market (NISM) or Association of Mutual Funds (AMFI) and have undergone the process of 'Know Your Distributor (KYD)', can perform the IPV.

V. However, in case of applications received by the mutual funds directly from the clients (i.e. not through any distributor), they may also rely upon the IPV performed by the scheduled commercial banks.

5.9. KYC & Anti Money Laundering/Counter-Financing of Terrorism (AML/CFT) — Guidelines for Insurers

Insurers offer a variety of products aimed at transferring the financial risk of a certain event from the insured to the insurer. These products include life insurance contracts, annuity contracts, non-life insurance contracts, and health insurance contracts. These products are offered to the public through trained agents of the insurance companies and also through a number of alternate distribution channels like direct marketing, bancassurance etc. The guidelines are therefore of importance to the agents and corporate agents also, to the extent indicated in the guidelines.
The obligation to establish an anti-money laundering program applies to an insurance company, and not to its agents, and other intermediaries. Hence the responsibility for guarding against insurance products being used to launder unlawfully derived funds or to finance terrorist acts, lies on the insurance company, which develops and bears the risks of its products.

Considering the potential threat of usage of the financial services by a money launderer, insurance company should make reasonable efforts to determine the true identity of customers. For the purposes of these norms, the term customer also refers to the proposer/policyholder; beneficiaries and assignee. Where a client is a juridical person, verification of identity is required to be carried out on persons purporting to act and is authorized to act on behalf of a customer. Special care has to be exercised to ensure that the contracts are not anonymous or under fictitious names.

1. Insurers shall verify and document identity, address and recent photograph (in case of individual customers) as part of compliance with KYC norms. A list of documents to be verified under KYC norms for individuals and others is given in Annexure I (which may be treated as illustrative only). No further documentation is necessary for proof of residence where the document of identity submitted also gives the proof of residence. Any document that is accepted by the Insurer should be such that it would satisfy regulatory/enforcement authorities, if need be at a future date that due

diligence was in fact observed by the insurer in compliance with the guidelines and the PML Act.

2. Insurance premium paid by persons other than the person insured should be looked into to establish insurable interest.
3. Care has to be exercised to avoid unwitting involvement in insuring assets bought out of illegal funds. It is imperative to ensure that the insurance being purchased is reasonable, especially in other than products like motor insurance that are mandated by law. Accordingly, customer's source of funds, his estimated net worth etc., could be documented where considered necessary. Proposal form may also have questionnaires/declarations on sources of fund. Insurers should take appropriate measures, commensurate with the assessed risk of customer and product profile as part of their due diligence measures which may include:

- conducting independent enquiries on the details collected on /provided by the customer where required,
- consulting a credible database public or other etc.,

4. Relevant records and details must be maintained in such a way that it enables verification at a later date and support the fact of having established sources of funds involved in the insurance contract.

5. At any point in time during the contract period, where an insurance company is no longer satisfied that it knows the true identity of the customer, an STR should be filed with FIU-IND.
6. Insurers are advised to maintain an updated list of designated individuals/entities in electronic form and run a check on the given parameters on a regular basis to verify whether designated individuals/ entities are holding any insurance policies with the company. An updated list of individual and entities which are subject to various sanction measures as approved by Security Council Committee established pursuant to UNSC 1267 can be accessed in the United Nations website at http://www.un.org/sc/committees/1267/consolist.shtml

7. Insurers are required to conduct detailed due diligence while taking insurance risk exposure to individuals/entities connected with countries identified by FATF as having deficiencies in their AML/CFT regime. Special attention should be paid to business relationships and transactions, especially those which do not have apparent economic or visible lawful purpose. In all such cases, the background and purpose of such transactions will as far as possible, have to be examined and written findings maintained for assisting competent authorities. Agents/ Corporate agents will have to be appropriately alerted to ensure compliance with this stipulation. While using the FATF Public Statements being circulated through the insurance councils, insurers should go beyond the FATF statements and consider publicly available information when identifying countries which do not or insufficiently apply the FATF Recommendations.
8. Similar measures shall be applied on countries considered as high risk from terrorist financing or money laundering perspective based on prior experiences, transaction history or other factors (e.g., legal considerations, or allegations of official corruption)

When should KYC be done?

Considering the vulnerability of general insurance products to threats of money laundering at the claims stage, general insurance companies are required to carry out KYC norms at the settlement stage where claim payout/premium refund crosses a threshold of ` One lakh per claim/premium refund. In cases where payments are made to third party service providers such as hospitals/ garages/ repairers etc., the KYC norms shall apply on the customers on whose behalf service providers act.

The AML/CFT checks become more important in case of claims on the policies assigned by the policyholder to a third party not related to him (except where the assignment is to Banks/FIs/Capital Market intermediaries regulated by IRDA/RBI/SEBI). Notwithstanding the above, insurers are required to ensure that no vulnerable cases go undetected. Especially where there is suspicion of money laundering or terrorist financing, or where there are factors to

indicate a higher risk, AML/CFT checks will have to be carried out on such assignments and STR should be filed with FIU-IND, if necessary.

Risk Assessment and Exempt Products:

The AML/CFT requirements focus on the vulnerability of the products offered by the insurers to any of the process of money laundering. Insurers shall carry out risk assessment of various products before deciding on the extent of due diligence measures to be applied in each case. An illustrative list of such vulnerable products/services are given in Annexure II

The hitherto, exempt standalone health/medi-claim policies shall also be brought under the purview of AML/CFT requirements based on the assessed risks associated with each of the product profile.

Based on the vulnerability criterion and after examining the product and business coverage the following products are exempt from the purview of AML/CFT requirements:

- Reinsurance and retrocession contracts where the treaties are between insurance companies for reallocation of risks within the insurance industry and do not involve transactions with customers
- Group insurance businesses which are typically issued (as per guidelines on group insurance policies) to a company, financial institution, or association and generally restrict the ability ofan individual insured / participant to manipulate

Implementation of Section 51A of UAPA:

By virtue of Section 51A of UAPA, the Central Government is empowered to freeze, seize or attach funds of and/or prevent entry into or transit through India any individual or entities that are suspected to be engaged in terrorism. To implement the said section an order reference F. No. 17015/10/2002-IS-VI dated 27th August, 2009 has been issued by the Government of India. The

salient aspects of the order with particular reference to insurance sector are detailed in the following paragraphs.

Communication under this section shall be addressed to Dr. Mamta Suri, Joint Director, Sectoral Development Department, Insurance Regulatory and Development Authority, 3rd Floor, Parishram Bhavan, Bashir Bagh, Hyderabad-500 004 E-mail: mamta@irda.gov.in; Telephone: 040 23381173; Fax: 040 6682 3334

A consolidated list of all the UAPA Nodal Officers of various agencies governed by the order will be circulated every year and on every change in the list, on receipt of the same from Ministry of Home Affairs.

i. Procedure for freezing of insurance policies of 'designated individuals/entities'

In case any matching records are identified, the procedure required to be adopted is as follows:

Insurance companies shall immediately and in any case within 24 hours from the time of identifying a match, inform full particulars of the insurance policies held by such a customer on their books to the Joint Secretary (IS-I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsis@nic.in.

The insurance companies shall also send a copy of the communication mentioned in 1.2(i) (a) above to the UAPA Nodal Officer of the State/UT where the account is held, IRDA and FIU-IND.

In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, insurance companies would prevent designated individuals/entities from conducting any transactions, under intimation to the Joint Secretary (IS-I), Ministry of Home Affairs at Fax no. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsis@nic.in.

The insurance companies shall file a Suspicious Transaction Report (STR) with FIU-IND in respect of the insurance policies covered by paragraph 1.2(i) (a) above, carried through or attempted, in the prescribed format.

On receipt of the particulars of suspected designated individual/entities IS-I Division of MHA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/entities identified by the insurance companies are the ones listed as designated individuals/entities and the insurance policies, reported by insurance companies are held by the designated individuals/entities.

In case, the results of the verification indicate that the insurance policies are owned by or are held for the benefit of the designated individuals/entities, an order to freeze these insurance policies under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned office of insurance company under intimation to IRDA and FIU-IND.

The said order shall take place without prior notice to the designated individuals/entities.

'Freezing of insurance contracts' would require not-permitting any transaction (financial or otherwise), against the specific contract in question.

Procedure for unfreezing of insurance policies of individuals/entities inadvertently affected by the freezing mechanism, upon verification that the individual/ entity is not a designated individual/entity

- Any individual or entity, if they have evidence to prove that the insurance policies, owned/held by them has been inadvertently frozen, shall move an application giving the requisite evidence, in writing, to the concerned insurance companies.

- The insurance companies shall inform and forward a copy of the application together with full details of the insurance policies inadvertently frozen as given by any individual or entity, to the Nodal Officer of IS-I Division of MHA within two working days.
- The Joint Secretary (IS-I), MHA, the Nodal Officer for IS-I Division of MHA shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within 15 working days, unfreezing the insurance policies owned/held by such applicant, under intimation to the concerned insurance company. However, if it is not possible for any reason to pass an Order unfreezing the assets within 15 working days, the Nodal Officer of IS-I Division shall inform the applicant.
- Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001 U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets, derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA Nodal Officer for IS-I Division for freezing of funds or other assets.
- The UAPA Nodal Officer of IS-I Division of MHA, shall cause the request to be examined, within 5 working days, so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the Nodal Officer in IRDA. The proposed designee, as mentioned above would be treated as designated individuals/entities.

- Upon receipt of the requests by these Nodal Officers from the UAPA Nodal Officer of IS-I Division, the list would be forwarded to insurance companies and the procedure as enumerated at paragraphs 1.2 (i) on freezing of insurance policies shall be followed.
- The freezing orders shall take place without prior notice to the designated persons involved.
- IRDA would communicate all Orders under section 51A of UAPA relating to insurance policies, to all the insurance companies after receipt of the same from IS-I Division of MHA.
- A list of individuals and entities subject to UN sanction measures under UNSC Resolutions (hereinafter referred to as 'designated individuals/entities') received from the Ministry of External Affairs (MEA) would be circulated to the insurance companies through the Councils.

Reporting Obligations:

The AML/CFT program envisages submission of Reports on certain transactions to a Financial Intelligence Unit-India (FIU-IND) set up by the Government of India to track possible money laundering attempts and for further investigation and action.

i. Suspicious Transactions Reports:

a. Suspicious activity monitoring program should be appropriate to the company and the products it sells. Special attention should be paid to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Background of such transactions, including all documents /office records /memorandums pertaining to such transactions, as far as possible, should be examined by the Principal Compliance Officer (refer para 2 (iii)) for recording his findings. These records are required to be preserved for ten years as indicated in clause 1.4.

An illustrative list of suspicious transactions is provided in Annexure-III.

Insurance companies should report the suspicious transactions immediately on identification. Such reports should include attempted transactions, whether or not made in cash, irrespective of the monetary value involved. When such transactions are identified post facto the contract, a statement may be submitted to FIU-IND within 7 working days of identification in the prescribed formats.

Directors, officers and employees (permanent and temporary) shall be prohibited from disclosing the fact that a Suspicious Transactions Report or related information of a policyholder/prospect is being reported or provided to the FIU-IND.

ii. Monitoring and Reporting of Cash Transactions:

a. With a view to ensuring that premiums are paid out of clearly identifiable sources of funds, premium/proposal deposits remittances in cash beyond ` 50000/- per transaction shall be accepted subject to the customer quoting PAN. Insurers shall verify the authenticity of the details of PAN so obtained. In case of customers not required to have PAN or with only agricultural income, Form 60/61 prescribed under the provisions of Income Tax Rules shall be obtained.

b. From the perspective of AML/CFT guidelines, it becomes imperative to obtain the details of PAN of the person/entity funding the premium/proposal deposit on an insurance policy.

c. Any cash transaction above ` 10 lakh and integrally connected cash transactions above ` 10 lakh per month shall be reported to FIU-IND by 15th of the succeeding month

d. Premium collected from various customers and remitted by intermediaries is however, excluded from these reporting requirements.

e. Insurers shall lay down proper mechanisms to check any kind of attempts to avoid disclosure of PAN details. In case of possible attempts to circumvent the requirements, the same shall be reviewed from the angle of suspicious activities and shall be reported to FIU-IND, if required.

f. The above clauses should not be selectively interpreted on individual transaction basis. Splitting of the insurance policies/issue of number of policies to one or more entities facilitating individuals to defeat the spirit of the AML/CFT guidelines should be avoided. Where there is possibility of transactions being integrated through a single remitter, the insurer should refuse to accede to the requests for cash deposits.

iii. Reporting of receipts by Non-Profit Organisations :

All transactions, involving receipts by non-profit organizations of value more than ` 10 lakh, or its equivalent in foreign currency, should be reported to FIU-IND by 15th day of next succeeding month.

iv. Reporting of Counterfeit Currency/Forged Bank notes (CCR):

All cash transactions, where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transaction should be reported within 7 days of identification to FIU-IND.

Record Keeping

- The insurer/agents/corporate agents are required to maintain the records of types of transactions mentioned under Rule 3 of PMLA Rules 2005 as well as those relating to the verification of identity of clients for a period of 10 years. The records referred to in

the said Rule 3 shall be maintained for a period of ten years from the date of transaction. Records pertaining to all other transactions, (for which insurance companies are obliged to maintain records under other applicable Legislations/ Regulations/ Rules) insurance companies are directed to retain records as provided in the said Legislation/Regulations/Rules but not less than a period of ten years from the date of end of the business relationship with the customer. Records can also be in electronic form.

- Sharing of information on customers may be permitted between different organisations such as banks, insurance companies, Income tax authorities, local government authorities on request.
- Insurance institutions should implement specific procedures for retaining internal records of transactions both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved (if any) so as to provide, if necessary, evidence for prosecution of criminal activity. In the case of long term insurance, full documentary evidence is usually retained based on material completed at the initiation of the proposal of the contract, together with evidence of processing of the contract up to the point of maturity.
- Companies should retain the records of those contracts, which have been settled by claim (maturity or death), surrender or cancellation, for a period of at least 10 years after that settlement.
- In situation where the records relate to ongoing investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed where practicable, insurance institutions are requested to seek and retain relevant identification documents for all such transactions and to report the offer of suspicious funds.
- In case of customer identification data obtained through the customer due diligence process, account files and business correspondence should be retained for at least 10 years after the business relationship is ended.

AML Compliance

Establishment of anti money laundering programs by financial institutions is one of the central recommendations of the Financial Action Task Force and also forms part of the Insurance Core Principles of the International Association of Insurance Supervisors (IAIS). Accordingly, IRDA (Insurance Regulatory and Development Authority) has put in place regulatory guidelines/ instructions to the Insurers, Agents and Corporate agents as part of the Programme on Anti Money Laundering/Counter-Financing of Terrorism (AML/CFT) for the insurance sector.
Anti Money Laundering/Counter-Financing of Terrorism (AML/CFT) — Guidelines for Insurers is covered under Master Circular IRDA/F&I/CIR/AML/158/09/2010, dated 24-9-2010 and AML/CFT Guidelines for General Insurers – IRDA/SDD/GDL//CIR/020/02/2013 dated 07-02-2013.

In order to discharge the statutory responsibility to detect possible attempts of money laundering or financing of terrorism, every insurer needs to have an AML/CFT program which should, at a minimum, include:

(*i*) Internal policies, procedures, and controls;

(*ii*) Appointment of a Principal compliance officer;

(*iii*) Recruitment and training of employees/agents;

(*iv*) Internal Control/Audit;

i) Internal policies, procedures, and controls

Insurance company should make reasonable efforts to determine the true identity of all customers requesting for its services especially the person who funds/pays for an insurance contract, either as beneficial owner or otherwise. For the purposes of these norms, the term customers also refer to the proposer/policyholder; beneficiaries and assignee. Where a client is a juridical person, verification of identity is required to be carried out on persons purporting to act and is authorized to act on behalf of a client. In case of new contracts, KYC should be done before the issue of every new insurance contract.

The degree of due diligence to establish KYC could be decided by the insurers where premium is below Rs. 1 lakh per annum. However, premium of Rs. 1 lakh per annum in case of individual business should be considered as a threshold for exercising detailed due diligence, whatever be the payment mode.

The insurer should not enter into a contract with a customer whose identity matches with any person with known criminal background or with banned entities and those reported to have links with terrorists or terrorist organizations.

In the context of the very large base of insurance customers and the significant differences in the extent of risk posed by them, the companies are advised to classify the customer into high risk and low risk, based on the individual's profile and product profile, to decide upon the extent of due diligence. Insurers should devise procedure to ensure that proposals for contracts with high risk customers are concluded after approval of senior management officials. It is however, emphasized that proposals of Politically Exposed Persons (PEPs) in particular requires approval of senior management, not below Head (underwriting)/Chief Risk Officer level.

The AML/CFT requirements focus on the vulnerability of the products offered by the insurers to any of the process of money laundering. Based on the vulnerability criterion and after examining the product and business coverage it has been decided that the following categories of products/business lines may be exempted from the purview of AML/CFT requirements:

(*i*) Standalone medical/health insurance products.

(*ii*) Reinsurance and retrocession contracts where the treaties are between insurance companies for reallocation of risks within the insurance industry and do not involve transactions with customers.

(*iii*) Group insurance businesses which are typically issued to a company, financial institution, or association and generally restrict the ability of an individual insured or participant to manipulate its investment.

(*iv*) Term life insurance contracts, in view of the absence of cash surrender value and stricter underwriting norms for term policies (especially those with large face amounts)

Suspicious activity monitoring program should be appropriate to the company and the products it sells. Special attention should be paid to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Background of such transactions, including all documents/office records/memoran-dums pertaining to such transactions, as far as possible, should be examined by the Principal Compliance Officer.

With a view to ensuring that premiums are paid out of clearly identifiable sources of funds, it has been decided that remittances of premium by cash should not exceed Rs. 50,000. It would be advisable for the companies to evolve even lower thresholds for cash transactions. Premium/proposal deposits beyond Rs. 50,000 should be remitted only through cheques, demand drafts, credit card or any other banking channels. For integrally related transactions, premium amount greater than Rs. 50,000 in a calendar month should be examined more closely for possible angles of money laundering. This limit will apply at an aggregate level considering all the roles of a single person-as a proposer or life assured or assignee.

All transactions, involving receipts by non-profit organizations (either in the form of assignments and/or in the form of top-up remittances) of value more than Rs. ten lakh, or its equivalent in foreign currency, should be reported to FIU-IND.

A detailed AML/CFT Policy should be drawn up encompassing aspects of Customer acceptance policy, Customer Identification procedure, Monitoring of transactions, Risk management framework as evolved by the insurer. The policy should have the approval of the board and duly filed with IRDA for information. The policy should be reviewed annually and changes effected based on experience.

ii) Appointment of a Principal compliance officer

The companies should designate a Principal Compliance Officer (PCO) under AML/CFT rules, at senior level and preferably not below the Head (Audit/Compliance)/Chief Risk Officer. The name of the principal compliance officer should be communicated to IRDA and FIU immediately.

- The Principal Compliance Officer should ensure that the Board approved AML/CFT program is being implemented effectively, including monitoring compliance by the company's insurance agents with their obligations under the program;

- He/She should ensure that employees and agents of the insurance company have appropriate resources and are well trained to address questions regarding the application of the program in light of specific facts.
- He/She should be able to act independently and report to senior management.
- He/She and staff assisting him in execution of AML/CFT guidelines should have timely access to customer identification data, other KYC information and records.

iii) Recruitment and Training of employees/agents

As most part of the insurance business is through agents/corporate agents which brings in non face to face business relationships with the policyholders, the selection process of agents/corporate agents should be monitored carefully. The committee monitoring the agents should monitor sales practices followed by agents and ensure that if any unfair practice is being reported then action is taken after due investigation; Periodic risk management reviews should be conducted to ensure company's strict adherence to laid down process and strong ethical and control environment. Insurance companies should have adequate screening procedures when hiring employees.

A general appreciation of the background to money laundering, and the subsequent need for identifying and reporting of any suspicious transactions to the appropriate designated point should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority. A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff. It will also be necessary to make arrangements for refresher training at regular intervals to ensure that staff does not forget their responsibilities. This might be best achieved by a twelve or six-monthly review of training. Timing and content of training packages for various sectors of staff will need to be adapted by individual insurance institutions for their own needs. Records of training imparted to staff in the various categories detailed above should be maintained.

iv) Internal Control/Audit

Insurance companies' internal audit/inspection departments should verify on a regular basis, compliance with policies, procedures and controls relating to money laundering activities. The

reports should specifically comment on the robustness of the internal policies and processes in this regard and make constructive suggestions where necessary, to strengthen the policy and implementation aspects. Exception reporting under AML/CFT policy should be done to Audit Committee of the Board.

Compliance Arrangements

i. A detailed AML/CFT Policy should be drawn up encompassing aspects of Customer acceptance policy, Customer Identification procedure, Monitoring of transactions, Risk management framework as evolved by the insurer. The policy should have the approval of the board. The policy should be reviewed annually and changes effected based on experience.

ii. Responsibility on behalf of the agents and corporate agents:

The guidelines place the responsibility of a robust AML/CFT program on the insurers. Nonetheless, it is necessary that steps are taken to strengthen the level of control on the agents and corporate agents engaged by the insurers.

a. A list of rules and regulations covering performance of agents and corporate agents must be put in place. A clause should be added making KYC norms mandatory and specific process document can be included as part of the contracts.

b. Services of defaulting agents who expose the insurers to AML/CFT related risks on multiple occasions should be terminated.

c. Insurance company when faced with a non-compliant agent or corporate agent should take necessary action to secure compliance, including when appropriate, terminating its business relationship with such an agent/corporate agent.

5.10. Anti Money Laundering/Counter-Financing of Terrorism (AML/CFT) – Guidelines for Postal schemes

The Department of Posts, Ministry of Communication & Information Technology has issued a master circular on KYC norms in Post Office Savings Bank and Savings Certificate under the AML/CFT regime.

The objective of KYC/AML/CFT guidelines is to prevent money laundering or terrorist financing activities by use of Post Office Savings Bank intentionally or unintentionally by criminal elements. KYC procedures also enable to post office Savings Banks to know/understand their customers better which in turn help them manage their risks prudently.

For the purpose of KYC policy, a customer is defined as:—

- An individual that maintains an account and/or has a cash certificate or has a business relationship with the Post Office Savings Bank.
- An individual on whose behalf the account is maintained (i.e. beneficial owner).

All Post Office Savings Banks should keep in mind that information collected from the customer for the purpose of opening of account or purchase of savings certificates is to be treated as confidential and details thereof are not to be divulged for cross selling or any other purposes.

KYC Policy

Under PMLA provisions, Post Office Savings Bank declares its KYC Policy on the following four elements:—

(*a*) Customer Acceptance Policy.

(*b*) Risk Management

(*c*) Customer Identification Procedure.

(*d*) Monitoring of Transactions; Record keeping and Reporting

Customer Acceptance Policy (CAP)

No account should be opened in anonymous or fictitious name/benami. Not to open an account or close an existing account where the Post Office Savings Bank is unable to apply appropriate Customer Due Diligence measures i.e. unable to verify the identity and/or obtain documents required as prescribed due to non- cooperation of the customer or non- reliability of

data/information furnished by the customer. However, the customer should not be harassed and any decision to close the account should be taken by head of the Postal Division by giving suitable notice to the customer.

Categorization of Customers i.e. Risk categorization

All customers according to the amount involved at the time of opening of account or purchase of Savings Certificates or credit into an existing account should be categorized with the perspective of risk involved, namely –

i. Low risk - Where the customer opens account or applies for purchase of certificates or applies for credit of maturity/prematurity value of any existing savings instrument with an amount up to Rs. 50,000/- and balance in all accounts and savings certificates does not exceed Rs. 50,000/-.

ii. Medium Risk - Where the customer opens account or applies for purchase of certificates or applies for credit of maturity/prematurity value of any existing savings instrument with an amount exceeding Rs. 50,000/- but up to Rs. 10 lakh and balance in all accounts and savings certificates does not exceed Rs. 10 lakh.

iii. High Risk - Where the customer opens account or applies for purchase of certificates or applies for credit of maturity/prematurity value of any existing savings instrument with an amount exceeding Rs.10 lakh and balance in all accounts and certificates does not exceed Rs.10 lakh.

Customer Identification Procedure

Following will be the CDD/KYC norms to be followed in case of opening of new accounts/purchase of certificates falling under different types of accounts or Savings Certificates –

FOR LOW RISK CATEGORIES

PHOTOGRAPH
One (two in case of EDBO) recent Passport Size Photographs are to be given.

<table>
<tr><td colspan="2">In case of Joint Account, photograph of all joint holders should be given.</td></tr>
<tr><td>IDENTIFICATION PROOF
Any one of the following documents</td><td>ADDRESS PROOF
Any one of the following documents for Address Proof</td></tr>
<tr><td>• Electoral Photo Identity card,
• Ration Card with photograph.
• Passport,
• Driving License,
• POSB Identity card/Post Office Identity Card, Identity card from Central/State Government or PSU e.g. PPO, BPL card, Job card issued under MG-NREGA duly signed by an officer of State Government.
• Photo Identity Card issued by recognized University/Education Board/College/School.
• The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number.</td><td>• Bank or Post Office Passbook/ Statement with current address
• Passport with current address.
• Ration Card with current Address.
• Electricity Bill of not more than three months old
• Telephone Bill of not more than three months old
• Salary Slip of reputed Employer with current address.
• Certificate from any Public Authority/Postman or Gram Dak Sewak Delivery Agent or Branch Postmaster.
• The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number.</td></tr>
<tr><td colspan="2">ATTESTATION OF PHOTOCOPY OF DOCUMENTS
Documents should be self-attested or in case of illiterate depositors should be attested by Gazetted Officer/Sarpanch/Branch/Sub/Head/Chief Postmaster or Postman/Gram Dak Sewak Delivery Agent. In case of investment through</td></tr>
</table>

agent, these documents should also be attested by the agent.
In case of Joint Account, ID and Address proof of all depositors are required.

FOR MEDIUM RISK CATEGORIES

PHOTOGRAPH One (two in case of EDBO) recent Passport Size Photographs are to be given. In case of Joint Account, photograph of all joint holders should be given.	
IDENTIFICATION PROOF Any one of the following documents	**ADDRESS PROOF** Any one of the following documents for Address Proof
• PAN card or letter issued by I T Authority quoting PAN or Declaration in Form 60 or 61. If only Declaration in Form 60 or 61 is provided then one of the following documents are to be given for Identification Proof. • Electoral Photo Identity card • The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number. • Passport, • Driving License, • Ration Card with photograph. • Photo Identity Card issued by recognized University/Education	• Bank or Post Office Passbook/ Statement with current address • Passport with current address. • Ration Card with current Address. • Electricity Bill of not more than three months old • Telephone Bill of not more than three months old • Salary Slip of reputed Employer with current address. • Certificate from any Public Authority/Postman or Gram Dak Sewak Delivery Agent or Branch Postmaster. • The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar

Board/College/School. • Identify card from Central/State Government or PSU.	number.
ATTESTATION OF PHOTOCOPY OF DOCUMENTS Documents should be self-attested or in case of illiterate depositors should be attested by Gazetted Officer/Sarpanch/Branch/Sub/Head/Chief Postmaster or Postman/Gram Dak Sewak Delivery Agent. In case of investment through agent, these documents should also be attestedby the agent.	
In case of Joint Account, ID and Address proof of all depositors are required.	

FOR HIGH RISK CATEGORIES

PHOTOGRAPH One (two in case of EDBO) recent Passport Size Photographs are to be given. In case of Joint Account, photograph of all joint holders should be given.	
IDENTIFICATION PROOF Any one of the following documents	**ADDRESS PROOF** Any one of the following documents for Address Proof
• PAN card or letter issued by IT Authority quoting PAN or Declaration in Form 60 or 61. If only Declaration in Form 60 or 61 is provided then one of the following documents are to be given for Identification Proof. • Electoral Photo Identity card • The letter issued by the Unique Identification Authority of India (UIDAI) containing details of	• Bank or Post Office Passbook/ Statement with current address • Passport with current address. • Ration Card with current Address. • Electricity Bill of not more than three months old • Telephone Bill of not more than three months old • Salary Slip of reputed Employer with current address. • The letter issued by the Unique Identification Authority of India

<table>
<tr><td>name, address and Aadhaar number.
• Ration Card with photograph.
• Passport,
• Driving License,
• Photo Identity Card issued by recognized University/Education Board/College/School.
• Identify card from Central/State Government or PSU.
Note: In case of SCSS account, where interest payment in exceeding Rs 10,000 in a financial year and declaration in Form 15G or 15H is not given, copy of PAN Card is mandatory.</td><td>(UIDAI) containing details of name, address and Aadhaar number.</td></tr>
<tr><td colspan="2">PROOF OF SOURCE OF FUND
The customer has to submit copy of document showing source of receipt of funds tendered for investment</td></tr>
<tr><td colspan="2">ATTESTATION OF PHOTOCOPY OF DOCUMENTS
Documents should be self-attested or in case of illiterate depositors should be attested by Gazetted Officer/Sarpanch/Branch/Sub/Head/Chief Postmaster or Postman/Gram Dak Sewak Delivery Agent. In case of investment through agent, these documents should also be attested by the agent.</td></tr>
<tr><td colspan="2">In case of Joint Account, ID and Address proof of all depositors are required.</td></tr>
</table>

SPECIAL CATEGORIES OF ACCOUNTS

PENSION ACCOUNT

<table>
<tr><td colspan="2">PHOTOGRAPH
One (two in case of EDBO) recent Passport Size Photographs are to be given. In case of Joint Account, photograph of all joint holders should be given.</td></tr>
<tr><td>IDENTIFICATION PROOF</td><td>ADDRESS PROOF
Any one of the following documents for Address Proof</td></tr>
<tr><td>Copy of PPO issued by competent Authority.</td><td>• Bank or Post Office Passbook/ Statement with current address
• Passport with current address.
• Ration Card with current Address.
• Electricity Bill of not more than three months old
• Telephone Bill of not more than three months old
• The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number
• Certificate from any Public Authority/Postman or Gram Dak Sewak Delivery Agent or Branch Postmaster.</td></tr>
<tr><td colspan="2">ATTESTATION OF PHOTOCOPY OF DOCUMENTS
Documents should be self-attested or in case of illiterate depositors</td></tr>
</table>

should be attested by Gazetted Officer/Sarpanch/ Branch/Sub/Head/Chief Postmaster or Postman/Gram Dak Sewak Delivery Agent. In case of investment through agent, these documents should also be attested by the agent.

WORKERS WAGE ACCOUNTS

PHOTOGRAPH One (two in case of EDBO) recent Passport Size Photographs are to be given. In case of Joint Account, photograph of all joint holders should be given.	
IDENTIFICATION PROOF	**ADDRESS PROOF** **Any one of the following documents for Address Proof**
Copy of JOB card issued under MG-NREGA duly signed by an officer of State Government.	▪ Bank or Post Office Passbook/ Statement with current address ▪ Ration Card with current Address. ▪ Electricity Bill of not more than three months old ▪ Telephone Bill of not more than three months old ▪ The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number ▪ Certificate from any Public Authority/ Postman or Gram Dak

	Sewak Delivery Agent or Branch Postmaster.
ATTESTATION OF PHOTOCOPY OF DOCUMENTS Documents should be self-attested or in case of illiterate depositors should be attested by Gazetted Officer/Sarpanch/ Branch/Sub/Head/Chief Postmaster or Postman/Gram Dak Sewak Delivery Agent. In case of investment through agent, these documents should also be attested by the agent.	

INDIRA GANDHI NATIONAL OLD AGE/WIDOW/DISABLED PENSION ACCOUNTS.

PHOTOGRAPH One (two in case of EDBO) recent Passport Size Photographs are to be given. In case of Joint Account, photograph of all joint holders should be given.	
IDENTIFICATION PROOF	**ADDRESS PROOF** **Any one of the following documents for Address Proof**
Copy of PPO issued by competent Authority.	• Ration Card with current Address. • Electricity Bill of not more than three months old • Telephone Bill of not more than three months old • The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and

	Aadhaar number • Certificate from any Public Authority/Postman or Gram Dak Sewak Delivery Agent or Branch Postmaster.
ATTESTATION OF PHOTOCOPY OF DOCUMENTS Documents should be self-attested or in case of illiterate depositors should be attested by Gazetted Officer/Sarpanch/ Branch/Sub/Head/Chief Postmaster or Postman/Gram Dak Sewak Delivery Agent. In case of investment through agent, these documents should also be attested by the agent.	

Note: In case where the account/certificate holder is minor, the norms shall be applicable to the guardian. In case of joint account, the norms will be applied for all the joint account/certificate holders.

When maturity value is credited into savings account

When any depositor or certificate holder requests for credit of maturity value into existing savings account, it should be allowed only after ensuring that concerned savings account was opened with due KYC documents applying risk category as per balance in the account after credit of maturity value. In case a new savings account is opened to credit maturity value, it should be ensured that due KYC documents of appropriate risk category are taken based on the maturity value being credited into the account.

General

In case any post office finds that depositor/investor is not co-operating in furnishing fresh KYC documents in case of any suspicion, the Postmaster will refer the matter to the head of Postal Division who will order closure of Account and intimate the depositor/investor the reasons of taking such decision.

In case, wife, son, daughter and parents etc. who live with the father/mother and son, as the case may be, ID proof and Address Proof of the relative with whom the prospective customer is living along with a declaration from the relative that the prospective customer who wants to open an account or purchase a certificate is staying with him/her.

Maintenance of Records of Transactions

All post offices shall maintain the record of all transactions including the record of:—

(*a*) All **cash** transactions of the value of more than Rs. 10 Lakh.

(*b*)All series of cash transactions which are less than Rs. 10 lakh but are integrally connected and are carried out within one month period and totally exceed Rs. 10 Lakh.

(*c*) Any transaction where cash is accepted and forged or counterfeit currency notes are used or where forgery of valuable Security or documents has taken place.

(*d*) Any attempted transaction involving forged or counterfeit currency notes, forged security or document.

(*e*) All suspicious transactions, involving deposit withdrawal, transfer of account, solvency certificate/Idemnity certificate etc. irrespective of the amount of transaction.

Reporting schedule

Types of Transactions	Method of reporting of transactions
Cash Transactions (CTR) (*a*) All cash transactions more than Rs. 10 Lakh. (*b*) All series of cash transactions which are less than Rs. 10 lakh but are integrally connected and are carried out within one month period and totally exceed Rs. 10 Lakh.	1. In-charge of every departmental post office will be personally responsible for preparation of list of transactions (deposit/issue/withdrawal/discharge) mentioning nature of transaction, amount, name and address of depositor/holder, date of transaction, place of

	transaction, PAN No. (if given) of depositor/holder. He/She will be responsible for sending this list to Head of the Division on monthly basis by 3rd working day of the subsequent month. 2. Head of the Division will be personally responsible for sending post office wise list of such transactions of his division to the Head of the circle by 5th working day of the subsequent month. 3. Head of the circle will be responsible for sending the consolidated post office-wise list of such transactions to DDG(PCO) in Directorate by 8th working day of the subsequent month. In case no such report is received from field units by due date, a NIL report should be sent to DDG (PCO), PMLA in Directorate.
Suspected Transaction (STR) (*c*) Any account where cash is accepted and forged or counterfeit currency notes are used or where forgery of	1. In-charge of every departmental post office will be personally responsible for preparation of list of transactions

valuable Security or documents has taken place. (*d*) Any attempted transaction involving forged or counterfeit currency notes, forged security or document. (*e*) All suspicious transactions, involving deposit withdrawal, transfer of account, solvency certificate/ Idemnity certificate etc. irrespective of the amount of transaction.	(deposit/issue/withdrawal/disc harge) mentioning nature of transaction, amount, name and address of depositor/holder, date of transaction, place of transaction, PAN No. (if given) of depositor/holder and nature/reson of suspicion in detail and will be responsible for sending this list to the Head of the Division (by name) on the very same day. 2. The Head of the Division will be personally responsible for sending post office wise list of such transactions of his division to head of circle (by name) on the very same day of the receipt of STR from PO. 3. The Head of the Circle will be responsible for sending the consolidated post office-wise list of such STRs to DDG(PCO), PMLA (by name) at Directorate by on the very same day of receipt of STR from D.O.

5.11 KYC in General

Knowledge about the client, customer, employee or person with whom any commercial transaction is done is important for everyone specially in today's time due to advancement of commerce and information technology.

1. KYC for Commercial Transaction

Know your customer (KYC) refers to relevant information from their clients for the purpose of doing business with them. Every business make due diligence of other company or business person before entering into any commercial transactions. In this process get details of company's including its management, products or services to make sure that party is creditworthy and have good standing in market place. Generally following procedure should be followed as part of KYC.

- Know the identity of company or person with whom business is to be done. Getting details of name, address and market report helps to know that prospective client is not a defaulting party.
- Third party reference gives more credibility about prospective client.
- Records obtained & communication made with prospective client should be maintained for future use. It sometimes helps as evidence in case of court cases.

2. KYC for Employer

Every employer hiring people through third party or under direct recruitment more or less makes due diligence of candidate before signing contract. It includes personal details of candidate, third part reference, family background, report of previous employer etc. This process is undertaken to know the identity about the candidate that helps in future in case something wrong is done by the employee.

3. KYC for general public

Due to risk of money or local law compliance, even a non-commerce person make identity of person with whom he/she is going to make any transaction either in money or in kind. Such process relives or somehow helps in fraud or cheating. It is suggested for every person to get the identity and location proof of person before any deal is taken place it may be sale of house, marriage, renting property, sale of asset etc.

6. EFFECT OF NON-COMPLIANCE

The socio-economic effects of money laundering are crippling. Illicit funds generated from criminal activities such as gun running, drug and human trafficking and other forms of organised crime is laundered into clean currency, and in turn used to fund new criminal operations or expand existing ones. This translates into more drug trafficking and dealing, more illegal firearms, more violent crimes, and – most disconcertingly – more international terrorism**.** Left unchecked, money laundering can undermine the integrity of entire financial systems, and embroil individual financial institutions in share-crippling financial scandals.

Moreover, the amounts of money generated from criminal activities and laundered throughout the world amount several billions of dollars – up to as much as 5% of the global GDP. This gives the beneficiaries of money laundering a lot of muscle, and certainly enough means to threaten political stability worldwide.

In essence, regulatory compliance seeks to curb this criminal proliferation by holding financial systems providers and banking institutions accountable for the financial activities of the clients they deal with. Money laundering poses a very real threat to the reputation and financial well-being of banks, law firms, accountants and asset management houses around the world, as these institutions are often unwitting accomplices in the laundering of dirty money.

Offence of and punishment for Money Laundering

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 will be guilty of offence of money-laundering. (Section 3 of PMLA, 2002)

Whoever commits the offence of money-laundering will be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to seven years and will also be liable to fine. But if the proceeds of crime involved in money laundering relates to any offence specified under paragraph 2 of Part A of the Schedule i.e. offences

specified under the Narcotic Drugs and Psychotropic Substances Act, 1985, then the term of imprisonment may extend to ten years. (Section 4 of PMLA, 2002)

Any person who willfully and maliciously gives false information and causes an arrest or a search to be made under this Act shall on conviction be liable for imprisonment for a term which may extend to two years or with fine which may extend to fifty thousand rupees or both. [Section 63(1) of PMLA, 2002]

If any person legally bound to give information relating to any offence of money laundering, refuses to answer any question put forth by the authorities or give evidence or produce books of accounts or other documents at a certain place or time, shall pay by way of penalty a sum which shall not be less than five hundred rupees but which may extend to ten thousand rupees for each such default or failure. [Section 63(2) of PMLA, 2002]

The offences under the Act will be cognizable and non-bailable.

Attachment of property involved in money laundering

Where the Director or any other officer not below the rank of Deputy Director authorised by the Director, has reason to believe (the reason for such belief to be recorded in writing), on the basis of material in his possession, that — any person is in possession of any proceeds of crime and such proceeds of crime are likely to be concealed, transferred or dealt with in any manner which may result in frustrating any proceedings relating to confiscation of such proceeds of crime, he may, by order in writing, provisionally attach such property for a period not exceeding 180 days from the date of the order.

No such order of attachment should be made unless, in relation to the scheduled offence, a report has been forwarded to a Magistrate under section 173 of the Code of Criminal Procedure, 1973, or a complaint has been filed by a person authorised to investigate the offence mentioned in that Schedule, before a Magistrate or court for taking cognizance of the scheduled offence, as the case may be, or a similar report or complaint has been made or filed under the corresponding law of any other country.

Notwithstanding anything contained above, any property of any person may be attached if the Director or any other officer not below the rank of Deputy Director authorised by him has reason

to believe (the reasons for such belief to be recorded in writing), on the basis of material in his possession, that if such property involved in money laundering is not attached immediately, the non-attachment of the property is likely to frustrate any proceeding under this Act.

Every order of attachment will cease to have effect after the expiry of 180 days from the date of the order or on the date of the order made by the Director, whichever is earlier.

The Director or any other officer who provisionally attaches the property should, within a period of 30 days from such attachment, file a complaint, stating the facts of such attachment before the Adjudicating Authority.

Process of Adjudication

Section 8 of PMLA, 2002 deals with the process of adjudication. On receipt of a complaint from the Director or any other officer who provisionally attaches any property or an application made by such officer for retention of seized record or property, the Adjudicating Authority may, on reason to believe that any person has committed an offence of money laundering or is in possession of proceeds of crime, serve a notice of not less than thirty days on such person calling upon him to indicate the sources of his income, earning or assets, out of which or by means of which he has acquired the property attached or frozen, the evidence on which he relies and other relevant information and particulars and show cause why all or any of such property should not be declared to be the properties involved in money laundering and confiscated by the Central Government. Where a notice specifies any property as being held by a person on behalf of any other person, a copy of such notice shall also be served upon such other person. Similar notice is required to be served on all persons when more than one person holds such property jointly.

Where on conclusion of a trial of an offence, the Special Court finds that the offence of money-laundering has been committed, it shall order that such property involved in the money-laundering or which has been used for commission of the offence of money-laundering shall stand confiscated to the Central Government.

Where on conclusion of a trial under this Act, the Special Court finds that the offence of money-laundering has not taken place or the property is not involved in money-laundering, it shall order release of such property to the person entitled to receive it.

Where the trial under the PML Act cannot be conducted by reason of the death of the accused or the accused being declared a proclaimed offender or for any other reason or having commenced but could not be concluded, the Special Court shall, on an application moved by the Director or a person claiming to be entitled to possession of a property in respect of which an order has been passed, pass appropriate orders regarding confiscation or release of the property, as the case may be, involved in the offence of money-laundering after having regard to the material before it.

7. FINANCIAL INTELLIGENCE UNITS (FIU)

One of the key elements of AML/CFT regimes is the requirement for financial institutions and other designated non-financial businesses (DNFBPs) to report transactions they deem suspicious of being related to criminal or terrorist activity. Because of confidentiality traditionally attached to financial transactions and because reporting entities do not always have the means to substantiate their suspicion, it proves difficult to report it directly to the authorities in charge of enforcing criminal laws. It is therefore necessary for governments to establish a specialized agency, the Financial Intelligence Unit (FIU), focused on processing financial information that may be related to criminal or terrorist activity.

In their simplest forms, FIUs are agencies that receive reports of suspicious transactions from financial institutions and other persons and entities, analyze them, and disseminate the resulting intelligence to local law-enforcement agencies and FIUs to combat money laundering. As government agencies, FIUs must retain sufficient independence to accomplish their objectives without undue interference or influence.

According to The Egmont Group, the informal international association of FIUs, 101 countries are currently recognized as operational FIU units, with others in various stages of development. The FATF 40+9 Recommendations call for countries to operate FIUs that meet the Egmont Group's definition.

The definition of an FIU has been formalized by the Egmont Group of FIUs as—

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

(*i*) Concerning suspected proceeds of crime and potential financing of terrorism, or

(*ii*) Required by national legislation or regulation in order to combat money laundering and terrorism financing"

Financial Intelligence Unit – India (FIU-IND) was set by the Government of India *vide* O.M. dated 18th November 2004 as the central national agency responsible for receiving, processing,

analyzing and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and related crimes. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister. For administrative purposes, FIU-IND is under the control of the Department of Revenue, Ministry of Finance.

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

- Combating money laundering, financing of terrorism and other economic offences;
- Deterring money laundering and financing of terrorism;
- Building and strengthening organisational capacity.

The main function of FIU-IND is to receive cash/suspicious transaction reports, analyse them and, as appropriate, disseminate valuable financial information to intelligence/enforcement agencies and regulatory authorities.

The functions of FIU-IND are—

- **Collection of Information:** Act as the central reception point for receiving Cash Transaction reports (CTRs) and Suspicious Transaction Reports (STRs) from various reporting entities;
- **Analysis of Information:** Analyze received information in order to uncover patterns of transactions suggesting suspicion of money laundering and related crimes.
- **Sharing of Information:** Share information with national intelligence/ law enforcement agencies, national regulatory authorities and foreign Financial Intelligence Units.
- **Act as Central Repository:** Establish and maintain national data base on cash transactions and suspicious transactions on the basis of reports received from reporting entities.

- **Coordination:** Coordinate and strengthen collection and sharing of financial intelligence through an effective national, regional and global network to combat money laundering and related crimes.
- **Research and Analysis:** Monitor and identify strategic key areas on money laundering trends, typologies and developments.

FIU-IND is a multi disciplinary body headed by the Director with a sanctioned strength of 74 personnel. These are being inducted from different organizations namely Central Board of Direct Taxes (CBDT), Central Board of Excise and Customs (CBEC), Reserve Bank of India (RBI), Securities Exchange Board of India (SEBI), Department of Legal Affairs and Intelligence agencies.

FIU-IND is not a regulatory authority. Its prime responsibility is to gather and share financial intelligence in close cooperation with the regulatory authorities including RBI, SEBI and IRDA. FIU-IND will process and analyse received financial information disseminate actionable intelligence in appropriate cases to relevant enforcement agencies.

FIUs exchange information with other FIUs on the basis of reciprocity or mutual agreement and consistent with procedures understood by the requested and requesting party. An FIU requesting information should disclose, to the FIU that will process the request, at a minimum the reason for the request, the purpose for which the information will be used and enough information to enable the receiving FIU to determine whether the request complies with its domestic law.

8. OTHER AUTHORITIES ENSURING IMPLEMENTATION OF ANTI-MONEY LAUNDERING MEASURES

1) Directorate of Enforcement (ED)

The ED has currently been entrusted with the investigation and prosecution of money-laundering offences and attachment/confiscation of the proceeds of crime under the Prevention of Money Laundering Act, 2002 (PMLA) apart from Foreign Exchange Management Act, 1999 (FEMA). The officers of the ED undertake multifaceted functions of collection, collation and development of intelligence, investigation into suspected cases of money laundering, attachment/confiscation of assets acquired through the commission of scheduled offences, and the criminal prosecution of the offenders in the court of law. The ED also enforces the provisions of FEMA, aimed at promoting the development and maintenance of India‘s foreign exchange market and providing, inter alia, for action against persons/entities involved in international hawala transactions.

The ED has a pan-Indian character with field offices spread over various states and regions. There is a separate legal wing headed by a Prosecutor, with two deputy legal advisers and 10 assistant legal advisers. The Directorate was restructured in March 2011 increasing the number of offices from 22 to 39 and the total strength of officers and staff to 2063. After the process of restructuring is completed, the Directorate will have headquarters in New Delhi, five regional offices at New Delhi, Mumbai, Kolkata, Chennai and Chandigarh, besides 11 zonal offices and 22 sub-zonal offices at various places.

The main functions of the Directorate are as under—

i. To initiate investigations under PMLA to ascertain whether proceeds of crime have been generated from the Scheduled offence booked by the concerned Law Enforcement Agency and such proceeds have been laundered. If a prima facie case of money laundering is made out, the Directorate attaches the property derived with/out of the proceeds of crime.

ii. To provide and seek mutual legal assistance to/from contracting states in respect of attachment/confiscation of proceeds of crime as well as in respect of transfer of accused persons under PMLA.

iii. To file prosecution complaints in the designated PMLA Court for the offence of money laundering under PMLA.

iv. To collect, develop and disseminate intelligence relating to contraventions of FEMA. The intelligence inputs are received from various sources such as Central and State Intelligence agencies, RBI, complaints, information gathered by officers, etc.

v. To investigate suspected contraventions of the provisions of FEMA relating to activities such as hawala, unauthorized dealings in foreign exchange, non-realization of export proceeds, unauthorized retention of funds abroad including bank accounts, unauthorized acquisition of immovable properties abroad, contraventions relating to Foreign Direct Investments (FDIs), External Commercial Borrowings (ECBs), Foreign Currency Convertible Bonds (FCCBs), etc.

vi. To adjudicate cases of violations of the erstwhile FERA, 1973 and FEMA, 1999.

vii. To realize penalties imposed on conclusion of adjudication proceedings.

viii. To handle appeals and prosecution cases under the erstwhile FERA, 1973.

ix. To handle appeals under FEMA.

x. To process and recommend cases for detention under the Conservation of Foreign Exchange and Prevention of Smuggling Activities Act (COFEPOSA) in respect of contraventions under FEMA.

2) Appellate Tribunal

The Appellate Tribunal under the Prevention of Money Laundering Act, 2002 (PMLA) was brought into force w.e.f. 1st July, 2005.

The Tribunal comprises a Chairman (who is or has been a Judge of the High Court or Supreme Court) and two members. One of the Members is an Accountant Member, who has been in the practice of accountancy as a Chartered Accountant for at least ten years and the other Member is

a person who is or has been a judge of a High Court or who is a member of India Revenue Service and has held the post of Commissioner/Joint Secretary or equivalent post in Indian Legal Service, Income Tax, Indian Economic Service, Indian Customs and Central Excise Service or Indian Audit and Accounts Service in that service for at least three years.

The Appellate Tribunal under PMLA is a National Tribunal having its headquarter at New Delhi. The Tribunal adjudicates appeals and allied petitions filed against the attachment/forfeiture orders passed by the Adjudicating Authority for attachment/forfeiture of properties involved in money laundering under PMLA. It also adjudicates appeals filed against the orders imposing fine passed by the Director- Financial Intelligence Unit India (FIU India). The Benches of the Appellate Tribunal sit at New Delhi without any benches elsewhere in the country.

The appeals and allied petitions are disposed off by the Benches as constituted by the Chairperson with one or two Members as the Chairperson may deem fit. During the period 1 April, 2011 to 15 December, 2011, 147 appeals and 133 miscellaneous petitions were filed and 13 appeals and 14 miscellaneous petitions were disposed.

9. INTERNATIONAL ORGANIZATIONS INVOLVED IN COUNTERING MONEY LAUNDERING

International efforts to combat financial system abuse, financial crime, and money laundering intensified in the late 1980s, sparked by the growing concerns about drug trafficking and the recognition that the internationalization of trade and finance and advancements in communication technology may facilitate money laundering. Since then, countering financial crime, and money laundering became an integral part of the agenda of many multilateral organizations.

The interagency response is led primarily by the Financial Action Task Force (FATF) and the affiliated regional organizations. Other international organizations, including those with a general mandate (such as the United Nations) and those with a specialized focus (particularly, the Financial Stability Forum and international standard-setting bodies of financial sector supervisors) also contribute.

1) FATF

The Financial Action Task Force (FATF), also known by its French name, Groupe d'action financière (GAFI), is an intergovernmental policy making body founded in 1989 on the initiative of the G7.

The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

The efforts of national law enforcement bodies on their own were deemed to be insufficient to deal with the wide geographical spread of the production and distribution activities of illegal narcotics and the ability to move drug money across borders. The problem required a multinational response. In response to mounting concern over money laundering, the Financial

Action Task Force on Money Laundering (FATF) was established by the G-7 Summit that was held in Paris in 1989. Recognising the threat posed to the banking system and to financial institutions, the G-7 Heads of State or Government and President of the European Commission convened the Task Force from the G-7 member States, the European Commission and eight other countries. (G-7 is a forum created by France in 1975, for the government of seven major economies namely Canada, France, Germany, Italy, Japan, the United Kingdom and the United States. In 1997, the group added Russia, thus becoming the G8.)

The primary policies issued by the FATF are the Forty Recommendations on money laundering and the 9 Special Recommendations (SR) on Terrorism Financing (TF).

The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. In collaboration with other international stakeholders, the FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. Starting with its own members, the FATF monitors countries' progress in implementing the FATF Recommendations; reviews money laundering and terrorist financing techniques and counter-measures; and, promotes the adoption and implementation of the FATF Recommendations globally.

The Task Force was given the responsibility of examining money laundering techniques and trends, reviewing the action which had already been taken at a national or international level, and setting out the measures that still needed to be taken to combat money laundering. In April 1990, less than one year after its creation, the FATF issued a report containing a set of *Forty Recommendations*, which were intended to provide a comprehensive plan of action needed to fight against money laundering.

In 1996 the Recommendations were revised for the first time to reflect evolving money laundering trends and techniques, and to broaden their scope well beyond drug-money laundering. In 2001, the development of standards in the fight against terrorist financing was

added to the mission of the FATF. In October 2001 the FATF issued the *Eight Special Rec*ommendations to deal with the issue of terrorist financing. The continued evolution of money laundering techniques led the FATF to revise the FATF standards comprehensively in June 2003. In October 2004 the FATF published a Ninth Special Recommendations, further strengthening the agreed international standards for combating money laundering and terrorist financing — the *40+9 Recommendations*.

In February 2012, the FATF completed a thorough review of its standards and published the revised FATF Recommendations. This revision is intended to strengthen global safeguards and further protect the integrity of the financial system by providing governments with stronger tools to take action against financial crime. They have been expanded to deal with new threats such as the financing of proliferation of weapons of mass destruction, and to be clearer on transparency and tougher on corruption. The 9 Special Recommendations on terrorist financing have been fully integrated with the measures against money laundering. This has resulted in a stronger and clearer set of standards.

The FATF Recommendations set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. Countries have diverse legal, administrative and operational frameworks and different financial systems, and so cannot all take identical measures to counter these threats. The FATF Recommendations, therefore, set an international standard, which countries should implement through measures adapted to their particular circumstances. The FATF Recommendations set out the essential measures that countries should have in place to:

- identify the risks, and develop policies and domestic coordination;
- pursue money laundering, terrorist financing and the financing of proliferation;
- apply preventive measures for the financial sector and other designated sectors;
- establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures;
- enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and

- facilitate international cooperation.

The FATF Standards are revised to strengthen the requirements for higher risk situations, and to allow countries to take a more focused approach in areas where high risks remain or implementation could be enhanced. Countries should first identify, assess and understand the risks of money laundering and terrorist finance that they face, and then adopt appropriate measures to mitigate the risk. The risk-based approach allows countries, within the framework of the FATF requirements, to adopt 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.

The measures set out in the FATF Standards should be implemented by all members of the FATF and the FSRBs (FATF-Style Regional Bodies), and their implementation is assessed rigorously through Mutual Evaluation processes, and through the assessment processes of the International Monetary Fund and the World Bank – on the basis of the FATF's common assessment methodology.

FATF Recommendations 2012 in a nutshell—

A – AML/CFT POLICIES AND COORDINATION

1 – Assessing risks & applying a risk-based approach

2 – National cooperation and coordination

B – MONEY LAUNDERING AND CONFISCATION

3 – Money laundering offence

4 – Confiscation and provisional measures

C – TERRORIST FINANCING AND FINANCING OF PROLIFERATION

5 – SRII Terrorist financing offence

6 – SRIII Targeted financial sanctions related to terrorism & terrorist financing

7 – Targeted financial sanctions related to proliferation

8 – Non-profit organisations

D – PREVENTIVE MEASURES

9 – Financial institution secrecy laws

Customer due diligence and record keeping

10 – Customer due diligence

11 – Record keeping

Additional measures for specific customers and activities

12 – Politically exposed persons

13 – Correspondent banking

14 – Money or value transfer services

15 – New technologies

16 – Wire transfers

Reliance, Controls and Financial Groups

17 – Reliance on third parties

18 – Internal controls and foreign branches and subsidiaries

19 – Higher-risk countries

Reporting of suspicious transactions

20 – Reporting of suspicious transactions

21 – Tipping-off and confidentiality

Designated non-financial Businesses and Professions (*DNFBPs*)

22 – DNFBPs: Customer due diligence

23 – DNFBPs: Other measures

E – TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS

24 – Transparency and beneficial ownership of legal persons

25 – Transparency and beneficial ownership of legal arrangements

F – POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES

Regulation and Supervision

26 – Regulation and supervision of financial institutions

27 – Powers of supervisors

28 – Regulation and supervision of DNFBPs

Operational and Law Enforcement

29 – Financial intelligence units

30 – Responsibilities of law enforcement and investigative authorities

31 – Powers of law enforcement and investigative authorities

32 – Cash couriers

General Requirements

33 – Statistics

34 – Guidance and feedback

Sanctions

35 – Sanctions

G – INTERNATIONAL COOPERATION

36 – International instruments

37 – Mutual legal assistance

38 – Mutual legal assistance: freezing and confiscation

39 – Extradition

40 – Other forms of international cooperation

The FATF currently comprises 34 member jurisdictions and 2 regional organisations, representing most major financial centres in all parts of the globe. India became member of the FATF in June 2010.

The FATF blacklist was the common shorthand description for the Financial Action Task Force list of "Non-Cooperative Countries or Territories" (NCCTs); i.e., countries which it perceived to be non-cooperative in the global fight against money laundering and terrorist financing. Although non-appearance on the blacklist was perceived to be a mark of approbation for Offshore Financial Centres (or "tax havens") who are sufficiently well regulated to meet all of the FATF's criteria, in practice the list included countries that did not operate as offshore financial centres. The FATF updates the blacklist regularly, designating countries to be added or deleted.

The term "non-cooperative" was sometimes criticized as misleading, as a number of the countries which appeared on the list simply lacked the infrastructure or resources to cope with relatively sophisticated financial criminals who try to operate there. Since 2008 the FATF has begun, at the behest of G20 leaders, a different and more analytical process of identifying countries and jurisdictions displaying strategic deficiencies in their anti-money laundering and anti-terrorist financing regimes.

A total of 17 countries were labelled as high-risk and non-cooperative jurisdictions by FATF as on February 2012.

2) Asia-Pacific Group on Money Laundering (APG)

The Asia/Pacific Group on Money Laundering (APG) is an international organisation (regionally focused) consisting of 41 members and a number of international and regional observers including the United Nations, IMF, FATF, Asian Development Bank and World Bank. All APG members commit to effectively implement the FATF's international standards for anti-money laundering and combating financing of terrorism referred to as the 40+9 Recommendations. Part of this commitment includes implementing measures against terrorists listed by the United Nations in the "1267 Consolidated List". The key functions of APG is to Assess APG members' compliance with the global AML/CFT standards through mutual evaluations; Coordinate technical assistance and training with donor agencies and APG jurisdictions to improve compliance with the AML/CFT standards; Co-operate with the international AML/CFT network; Conduct research into money laundering and terrorist financing methods, trends, risks and vulnerabilities; Contribute to the global AML/CFT policy development by active Associate Membership of FATF.

.

3) The Egmont Group Financial Intelligence Units (FIUs)

The fight against money laundering has been an essential part of the overall struggle to combat illegal narcotics trafficking, the activities of organised crime, and more recently the financing of terrorist activity. It became obvious over the years that banks and other financial institutions were an important source for information about money laundering and other financial crimes

being investigated by law enforcement. Concurrently, governments around the world began to recognise the virulent dangers that unchecked financial crimes posed to their economic and political systems. To address that threat, a number of specialized governmental agencies were created as countries around the world developed systems to deal with the problem of money laundering. These entities are now commonly referred to as "financial intelligence units" or "FIUs". They offer law enforcement agencies around the world an important avenue for information exchange.

Recognizing the benefits inherent in the development of a FIU network, in 1995, a group of FIUs at the Egmont Arenberg Palace in Brussels decided to establish an informal group for the stimulation of international co-operation. Now known as the Egmont Group, these FIUs meet regularly to find ways to cooperate, especially in the areas of information exchange, training and the sharing of expertise.

Countries must go through a formal procedure established by the Egmont Group in order to be recognised as meeting the Egmont Definition of an FIU. The Egmont Group as a whole meets once a year. Since the Egmont Group is not a formal organisation, there is no permanent secretariat. Administrative functions are shared on a rotating basis. Aside from the Egmont Support position, Working Groups and the Egmont Committee are used to conduct common business.

One of the main goals of the Egmont Group is to create a global network by promoting international co-operation between FIUs.

As of 2011, there are 117 members in the Egmont Group.

4) United Nations Office on Drugs and Crime (UNODC)

The United Nations Office on Drugs and Crime (UNODC) is a United Nations office that was established in 1997 as the Office for Drug Control and Crime Prevention by combining the United Nations International Drug Control Program (UNDCP) and the Crime Prevention and Criminal Justice Division in the United Nations Office at Vienna. It is a member of the United Nations Development Group and was renamed the United Nations Office on Drugs and Crime in 2002. The agency is headquartered in Vienna, Austria.

These are the main themes that UNODC deals with: Alternative Development, Corruption, Criminal Justice, Prison Reform and Crime Prevention, Drug Prevention, -Treatment and Care, HIV and AIDS, Human Trafficking and Migrant Smuggling, Money Laundering, Organized Crime, Piracy, Terrorism Prevention.

The Law Enforcement, Organized Crime and Anti-Money-Laundering Unit of UNODC is responsible for carrying out the Global Programme against Money-Laundering, Proceeds of Crime and the Financing of Terrorism, which was established in 1997 in response to the mandate given to UNODC through the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988. The Unit's mandate was strengthened in 1998 by the Political Declaration and the measures for countering money-laundering adopted by the General Assembly at its twentieth special session, which broadened the scope of the mandate to cover all serious crime, not just drug-related offences. The broad objective of the Global Programme is to strengthen the ability of Member States to implement measures against money-laundering and the financing of terrorism and to assist them in detecting, seizing and confiscating illicit proceeds, as required pursuant to United Nations instruments and other globally accepted standards, by providing relevant and appropriate technical assistance upon request.

5) International Money Laundering Information Network (IMoLIN)

The International Money Laundering Information Network (IMoLIN), a one-stop AML/CFT research resource, was established in 1998 by the United Nations on behalf of a partnership of international organizations involved in anti-money laundering. The Global Programme against Money Laundering, Proceeds of Crime and the Financing of Terrorism (GPML) of the United Nations Office on Drugs and Crime (UNODC) now administers and maintains IMoLIN on behalf of the following 11 partner organizations: the Asia Pacific Group on Money Laundering (APG), the Caribbean Financial Action Task Force (CFATF), the Commonwealth Secretariat, the Council of Europe — MONEYVAL, the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), the EuroAsian Group (EAG), the Financial Action Task Force (FATF), the Financial Action Task Force on Money Laundering in South America (GAFISUD), the Inter-Governmental Action Group Against Money Laundering in West Africa (GIABA), Interpol, and the Organization of American States (OAS/CICAD). In the first half of 2004,

GPML relaunched IMoLIN, after completing an extensive renovation of the site's 'look and feel' and its content, in collaboration with UNODC's IT Section.

This multi-faceted website serves the global anti-money laundering community by providing information about national money laundering and financing of terrorism laws and regulations and contacts for inter-country assistance. Inter alia, it identifies areas for improvement in domestic laws, countermeasures and international co-operation. Policy practitioners, lawyers and law enforcement officers all regularly use IMoLIN as a key reference point in their daily work. The information on IMoLIN is freely available to all Internet users, with the exception of AMLID, which is a secure database.

10. ANTI-MONEY LAUNDERING MEASURES TAKEN AROUND THE WORLD

1) South Africa

The Financial Intelligence Centre Act (38 of 2001) (the FIC Act) came into effect on the 1st of July 2003. The FIC Act was introduced to fight financial crime, such as money laundering, tax evasion, and terrorist financing activities.The FIC Act brings South Africa in line with similar legislation in other countries designed to reveal the movement of monies derived from unlawful activities and thereby curbing money laundering and other criminal activities.

The Purpose of the Financial Intelligence Centre Act is to: assist in the identification of the proceeds of unlawful activities; combat money laundering; and combat the financing of terrorist and related activities. The Act does this by creating a legal framework for effective identification and verification of client identities; recordkeeping; reporting processes; staff training; compliance requirements and the establishment of the Financial Intelligence Centre and Counter-Money Laundering Advisory Council.

2) USA

Pursuant to the USA Patriot Act of 2001, the Secretary of the Treasury was required to finalize regulations before October 26, 2002 making KYC mandatory for all US banks. The related processes are required to conform to a customer identification program (CIP)

The USA PATRIOT Act is an Act of Congress that was signed into law by President George W. Bush on October 26, 2001. The title of the act is a ten-letter acronym (USA PATRIOT) that stands for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

Title III of the Act, titled "International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001," is intended to facilitate the prevention, detection and

prosecution of international money laundering and the financing of terrorism. It primarily amends portions of the Money Laundering Control Act of 1986 (MLCA) and the Bank Secrecy Act of 1970 (BSA). It was divided into three subtitles, with the first dealing primarily with strengthening banking rules against money laundering, especially on the international stage. The second attempts to improve communication between law enforcement agencies and financial institutions, as well as expanding record keeping and reporting requirements. The third subtitle deals with currency smuggling and counterfeiting, including quadrupling the maximum penalty for counterfeiting foreign currency.

The first subtitle tightened the record keeping requirements for financial institutions, making them record the aggregate amounts of transactions processed from areas of the world where money laundering is a concern to the U.S. government. It also made institutions put into place reasonable steps to identify beneficial owners of bank accounts and those who are authorized to use or route funds through payable-through accounts. The U.S. Treasury was charged with formulating regulations intended to foster information sharing between financial institutions to prevent money-laundering. Along with expanding record keeping requirements it put new regulations into place to make it easier for authorities to identify money laundering activities and to make it harder for money launderers to mask their identities. If money laundering was uncovered, the subtitle legislated for the forfeiture of assets of those suspected of doing the money laundering. In an effort to encourage institutions to take steps that would reduce money laundering, the Treasury was given authority to block mergers of bank holding companies and banks with other banks and bank holding companies that had a bad history of preventing money laundering. Similarly, mergers between insured depository institutions and non-insured depository institutions that have a bad track record in combating money-laundering could be blocked.

Restrictions were placed on accounts and foreign banks. It prohibited shell banks that are not an affiliate of a bank that has a physical presence in the U.S. or that are not subject to

supervision by a banking authority in a non-U.S. country. It also prohibits or restricts the use of certain accounts held at financial institutions.

3) NEW ZEALAND

Updated KYC laws were enacted in late 2009, and entered into force in 2010. KYC is mandatory for all registered banks and financial institutions (the latter being given an extremely wide meaning). New Zealand's Anti-Money Laundering/Counter-Terrorist Financing Act of 2009 sets reporting requirements for financial service providers and casinos and establishes a risk-based approach to tracking potential money laundering and terrorism financing activities.

The following is a list of Know Your Customer entities covered by New Zealand Law:

- Banks exchange offices, and money service businesses
- Credit card companies
- Mortgage lenders
- Casinos
- Securities brokers/dealers
- Safekeeping providers
- Asset and individual or collective portfolio managers
- Life insurance or other investment related insurance

As per section-11 A reporting entity must conduct customer due diligence on—

- a customer:
- any beneficial owner of a customer:
- any person acting on behalf of a customer.

A customer who is an individual and who the reporting entity believes on reasonable grounds is not acting on behalf of another person is to be treated as if he or she were also the beneficial owner unless the reporting entity has reasonable grounds to suspect that that customer is not the beneficial owner.

4) PAKISTAN

Pakistan's anti-money laundering laws consist of Anti-Money Laundering Ordinance, 2007 and Anti-Money Laundering Regulations 2008.

The Anti-Terrorism Act of 2002 defines the crimes of terrorist finance and money laundering and establishes jurisdictions and punishments. The National Accountability Ordinance of 1999, which requires financial institutions to report suspicious transactions to the NAB and establishes accountability courts; and The Control of Narcotic Substances Act of 1997, which also requires the reporting of suspicious transactions to the ANF, contains provisions for the freezing and seizing of assets associated with narcotics trafficking, and establishes special courts for offenses (including financing) involving illegal narcotics. All these laws include provisions to allow investigators to access financial records and conduct financial investigations.

The Anti-Money Laundering Act, provides for the prevention of money laundering (AML) and combating financing of terrorism (CFT) in Pakistan. Among other provisions, the act:

- Establishes a National Executive Committee to make high-level decisions on AML/CFT matters;
- Establishes a Financial Monitoring Unit (FMU) to receive and analyze reports of suspicious transactions, assist in investigations, recommend changes to regulations, and generally exercise responsibility for AML/CFT; and
- Provides directions on investigation, search and seizure of property.

5) JAPAN

Based on the revisions of the FATF 40 Recommendations in 2003, Japan enforced the 'Act on Prevention of Transfer of Criminal Proceeds' in 2007. The act has been amended on 28 April 2011 effective from 1 April 2013. Several other laws implemented for Anti-Money Laundering measures include the following:

a) Anti-Drug Special Prevention Law (1992)

b) Act on the Punishment of Organized Crime (2000).

Customer identification and verification for a variety of occasional transactions above the designated threshold of JPY 2,000,000 is required under Article 8, paragraph 1 (i) (p) of the Order for Enforcement of the Act. The threshold is lowered to JPY 100,000 for wire transfers. The listing of occasional transactions covered by this provision is comprehensive and includes transactions "for receiving and paying cash, a check to bearer, cashier's check or a certificate or coupon of a public or corporate bearer bond" as well as the exchange of Japanese or foreign currencies and the purchase or sale of traveler's checks.

Specified Business Operators are required to verify a natural person's name and domiciliary address and date of birth by reviewing the customer's driver's license or by "any other method specified by an ordinance of the competent ministries." Specified Business Operators are required to verify the name and location of the head or main office of a legal person using a certificate of registered matters, seal registration certificate or any other document issued by a "public agency" which includes this information.

6) CHINA

The primary legislation governing AML in China as follows:

a) Anti-money Laundering Law (2006)
b) Provisions on Anti-money Laundering through Financial Institutions (2006)
c) Administrative Measures for Financial Institutions on Report of Large-sum Transactions and Doubtful Transactions (2006)
d) Administrative Measures for Financial Institutions on Report of Transactions Suspected of Financing for Terrorist Purposes (2007)
e) Administrative Measures for Financial Institutions on Identification of Client Identity and Preservation of Client Identity Materials and Transactions Records (2007).

11. CASE STUDIES OF MONEY LAUNDERING

Various modes of money laundering carried out around the world is discussed in the cases hereunder.[2]

I. Underground banking/alternative remittance services/hawala

1. The Australian Crime Commission (ACC), together with its partners, had identified ongoing vulnerability of exploitation by organised crime in the alternative remittance sector and produced jointly with AUSTRAC (Australia's anti-money laundering & counter terrorism financing regulator) a strategic assessment that analysed the extent of criminal exploitation by, and of, alternative remittance service providers. This represented a challenge to law enforcement nationally.

   Through this ACC-led joint investigation with Victoria Police, the services of a remittance business based in Melbourne and Vietnam were targeted for money laundering activities. The operator of this business is alleged to have been responsible for laundering illicit profits on behalf of high-level drug trafficking groups.

   The investigation resulted in the seizure of cash and drugs during July, August and September 2011 including some $2.5 million (USD 2,379,960) in cash, just over one kilogram of cocaine, over 26.3 kilograms of heroin and 9.4 kilograms of methyl amphetamine. Eleven people were arrested for a variety of offences including trafficking drugs, money laundering and possessing the proceeds of crime.

2. From January 2008 to October 2010, Mr Lee and Mr Liao operated cross-strait underground banking between Mainland China and Chinese Taipei which violated the Banking Act. Mr Lee directed Mr Liao to inform the clients to deposit funds into the accounts of Mr A, B & C in Bank X, the accounts of Mr D, E & F in Bank Y and the accounts of Mr H & I in Bank Z which were controlled by Mr Liao. Then Mr Liao would

[2] Source – APG Yearly Typologies Report, 2013

inform Mr Lee to deposit the equivalent RMB to the bank accounts in Mainland China designated by the clients. Mr Lee and Mr Liao checked the information of clients and the remitting details by fax every day. Mr Lee paid Mr Liao NTD35,000 (about USD1,666) per month while Mr Liao paid bona fide Ms Ye as reward for operating the abovementioned bank accounts by case. During the period, Mr Lee and Mr Liao operated cross-strait underground banking totalling up to NTD 5,110,867,700 (about USD 170,362,256). This case was investigated by the Taipei Field Division of the Investigation Bureau and the abovementioned suspects were charged with violation of the Banking Law by the prosecutor of the Shi-Lin District Prosecutors Office in June 2011.

3. Mr Tsai and Mr Chen were respectively a representative and a staff member of Lung X International Trading Company. Chen and Tsai were aware that only banks may conduct transactions related to domestic and international currencies. Since 2005, they illegally used the accounts of 16 individuals, including Mr Hung, to operate underground currency exchange business and collected NTD2,000 (about USD67) processing fee for every RMB100,000 (about USD16 thousand). The total transactions in and out of these accounts amounted to over NTD7,898 million (about USD 236 million). The Investigation Bureau referred the case to Taipei District Prosecutor's Office for further investigation on 26 August 2011.

4. A group of people with foreign currency was intercepted by enforcement agencies. These people led the agency to another Person "B" who was to be given that currency. Person B further led them to Person "M". During a search certain documents were recovered and it was found that Person M was dealing in unauthorized exchange of currency through a network of people who were acting as his branches. The transactions were only in the currency of a particular jurisdiction. The people of the other jurisdiction came to this jurisdiction. They exchanged currency through Person M and his network which they use to buy goods and take to their homeland through different channels. Similarly some traders from this jurisdiction went to buy goods from the other jurisdiction for which they

took the currency of the other jurisdiction from person M. A branch-wide account was also maintained.

II. Use of offshore banks and international business companies, offshore trusts

1. In December 2011 the General Intelligence Agency (GIA) of Mongolia detained citizens of Belarus "O" and "S" who were residing in Mongolia and who opened over 50 accounts in one of the Mongolian commercial banks. In order to open such numerous accounts "O" and "S" established seven representative offices of UK and Russian companies and 8 legal entities in Mongolia. The Mongolian bank opened accounts based on the furnished documents, including an investment agreement for geological exploration. Under this investment agreement during the two year period from 2009 to 2011, 4.3 billion roubles (USD 160 million) was received from a private Russian commercial bank "S".

   The Mongolian bank informed "O" and "S" on every occasion about the rouble transactions from Russia. Then all the received roubles were converted into dollars and euros and placed into the accounts of the above-mentioned companies to obfuscate its origin. After numerous, confusing, domestic transactions all the money finally converged in the account of a UK registered company "F". Company "F", operating as a foreign trading company's representative office in Ulaanbaatar, transferred dollars and euros as a payment for loans and textile equipment to Cyprus, Latvia, Lithuania, Turkey, British Virgin Islands and 15 other countries.

   Eventually, investigators revealed that the money was never used under the investment agreement for geological exploration; everything was transferred to foreign countries. The private Russian commercial bank was announced as a bankrupt in December 2010, the UK registered company "F" was a shell company which was liquidated in 2009, all documents provided by citizens of Belarus were false and almost all recipients of the money in Cyprus, Latvia, and British Virgin Islands were Russian citizens.

III. Use of Professional Services (lawyers, accountants)

1. In the course of investigation by Japan Police of loan-sharking cases, it was found that a large amount of criminal proceeds had been transferred to the bank accounts of various companies which were identified as shell companies. It was also revealed that a certified administrative procedures specialist was involved in the creation of the companies which had Boryokudan gangsters on their board of directors. Upon receiving requests from customers, mainly through the Internet, which was on a non-face-to-face basis, the specialist prepared the articles of the company and other application documents without conducting appropriate customer identification. The number of transactions involving the specialist from 2008 to 2011 was at least over 1,000 cases.

   While Japan Police arrested several suspects for violation of the Act on Punishment of Organized Crimes, as they concealed about 370 million yen (about USD 47 million) from March 2011 to Feb 2012, they failed to arrest the certified administrative procedures specialist for the charge as an accomplice because he insisted that he had never been aware of the plot of the customers.

   However, the investigation succeeded in taking the case to prosecution for violation of the Act of certified administrative procedures specialists in March 2012, by looking at the fact that he had not maintained records adequately. In addition to the criminal charge, an administrative order was delivered by the prefectural governor who supervised the certified administrative procedures specialist, based on the Act on Prevention of Transfer of Criminal Proceeds in July 2012 for failing to take adequate measures for customer identification and record keeping.

2. An Australian-based mining company initiated an internal investigation after it was suspected an employee had stolen more than AUD1.1 million over a three-year period. The company identified the suspect through internal audit processes and the matter was referred to law enforcement authorities for further investigation. The law enforcement investigation revealed that the suspect, an accountant employed by the company, had abused his position of trust by systematically making a series of unauthorised international transfers over a three-year period. The transfers were made from a company

account to a number of offshore accounts held in the suspect's name and a number of his family members' names. An STR submitted by a bank suggested that an outgoing funds transfer of AUD27,500 from the suspect's personal account appeared to be sourced from company funds. The suspect was the beneficiary of the outgoing transfer and bank staff noticed that four days prior to the transfer, the exact amount of AUD27,500 was transferred into the suspect's account from a company account. AUSTRAC analysis found a number of transaction reports linked to the suspect. These supported the allegation of theft and identified the significant extent of the financial activity undertaken by the suspect. AUSTRAC information revealed that the suspect was the beneficiary of 17 outgoing IFTIs to India in amounts of between AUD2,400 and AUD33,400. Funds were sent from either the suspect's personal Australian-based bank account or from the company's account. In total, approximately AUD300,000 was transferred, all believed to be the proceeds of the theft. Law enforcement officers contacted the suspect while he was overseas. The suspect surrendered to authorities on his return to Australia. The suspect was charged with 10 counts of stealing and sentenced to seven years imprisonment. After serving four years the suspect was deported from Australia.

The jurisdictions involved were Australia and India. Indicators in the case included:

- Customer receiving multiple large-value domestic transfers into their personal account from a company account, followed by an outgoing international funds transfer equivalent in value to the domestic transfer.
- International funds transfers from an individual's account to several offshore accounts held in the same name.
- International funds transfers inconsistent with transaction history.

IV. Real estate

1. Approximately 60 bank deposits of amounts less than AUD10,000 were deposited into an individual's account within a four-month period, totalling AUD550,000. Money was also deposited at a credit union. Following this series of structured deposits into the accounts,

the individual in question purchased three real estate properties with bank cheques, and a high-value motor vehicle with AUD66,900 cash. It is not known how the significant amount of cash required to pay for the car was delivered to the motor vehicle dealer, but it was withdrawn from a bank account and paid to the dealer in two installments. A law enforcement investigation commenced and the suspect was eventually charged with supplying prohibited drugs and money laundering offences, and approximately AUD1.5 million worth of assets have been restrained.

V. Trade based money laundering and transfer pricing

1. Mr Chang was the nominal owner of Company A which was controlled by Mr Chen. Mr Lin was the owner of Company B and he designated a mainlander, Ms Qu, as the nominal owner of Company B, registered in Marshall Islands and designated an American, Mr Joseph, as the nominal owner of Company C registered in B.V.I. In March 2008, Mr Chen and Mr Chang considered that the solar energy industry was going to have a booming future. Thus they decided to cooperate with Mr Lin and invest NTD500 million (about USD17 million) into Company B in the name of Company A to run a production line of solar energy equipment. They then planned to manipulate the stock price of Company B and undertake an insider trading scheme. Considering that Company A only had funds of no more than NTD100 million (about USD3.3 million), they created the illusion of investing an amount of NTD500 million by transferring NTD100 million from Company A's account in Bank M to the Company B's account in Bank X, then to Company C's account in Bank Y in the Marshall Islands, then to Bank D's account in Bank Z in B.V.I. and then back to the account of Company A.

   They remitted funds this way five times from July to September 2012, which made it appear that Company A invested NTD500 million in Company B. After the last time the funds of NTD100 million were transferred to the account of Company B, Mr Chen withdrew them by cash and deposited this into several of his nominal accounts to manipulate the stock price of the company.

The stock prices of company B were successfully manipulated from NTD6 to NTD 19 per stock, booming more than three times. Meanwhile, Mr Lin and his wife, Mrs Liu, a teacher at an elementary school, used their personal account in Bank X and those of Teacher Ding and Teacher Chen, who were Mrs Liu's colleagues, to buy the stocks of Company B with NTD10 million (about USD333 thousand) to undertake insider trading and they gained more than NTD20 million (about USD666 thousand).

In December 2008, the Taipei Field Division of the Investigation Bureau received a letter of accusation and began an investigation. AMLD also received an STR from Bank X indicating that the bank account of Company B was usually operated by the employees of Company A including withdrawals and deposits in cash. AMLD disseminated the information to the Taipei Field Division of the Investigation Bureau.

In February 2011, the abovementioned suspects were all charged with embezzlement of the company's assets and manipulating the stock prices. Mr Chen and Mr Chang were prosecuted by the Taipei District Prosecutors Office and sentenced to 12 years and Mr Lin was prosecuted and sentenced to 10 years, all were fined NTD100 million (about USD3.3 million). In April 2012, Mr Lin and his wife, Mrs Liu were charged with insider trading and the prosecutor also appealed to confiscate the proceeds of crime amounting to NTD20 million (about USD666 thousand).

2. Searches were conducted on the premises of X Group of Companies and resulted in the seizure of incriminating documents as well as huge amounts of cash, indicating the supply of diamonds in dubious trades which were only on paper, with bills/invoices being issued for only nominal commission without supplying diamonds.

   The foreign inward remittances, in the guise of advances for exports, were received from persons other than buyers. These were for the purpose of channelling the funds parked abroad in the guise of export proceeds. The suspected hawala transactions were carried out and the funds received from abroad were diverted to activities other than those relating to exports and included large scale investment in real estate. The company is involved in money-laundering (including cross-border) and accounts in foreign jurisdictions have been traced and frozen.

VI. Use of nominees, trusts, family members or third parties

1. AUSTRAC information assisted a law enforcement investigation that led to the arrest of a suspect who had laundered a significant amount of cash raised through drug trafficking. The investigation found the suspect had used a variety of methods to launder the money:

    - The suspect arranged for a family member to deposit the illicit cash into a number of different bank accounts held by that family member.
    - The accounts were held at a number of different institutions to avoid arousing the suspicion of any one financial institution.
    - To further avoid scrutiny, the cash deposits were structured to fall below the AUD10,000 transaction reporting threshold.
    - The suspect then purchased a legitimate business and established an associated corporation.
    - The proceeds of crime were periodically withdrawn by cheque from the family member's accounts and deposited into the company account operated by the suspect.
    - The cheque deposits were subsequently explained by the suspect as being a loan from the family member to pay the purchase price of the business.
    - More than AUD420,000 was laundered using these techniques.

    The investigation also uncovered more than AUD650,000 in cash that the offender had hidden in a shed. Law enforcement officers ultimately charged the suspect with money laundering.

2. The Cybercrime Unit of the Fiji Police Force received two reports last year whereby a total of $12,500 (USD6,782) was illegally transferred from a business bank account to another unrelated account in the same bank. The money was withdrawn by the account holder and handed over to a third party (suspect) who, after taking his share remitted the balance of the funds to Nigeria. The suspect sent about $8,000 (USD4,340) from a

foreign exchange dealer on different occasions over a period of five days. The suspect used the identification (ID) of various third parties and managed to remit the funds to Nigeria. The remittances were reportedly facilitated by the money remittance agency who allowed the suspect to remit the funds using different names and identification (in the absence of the ID owners) to different beneficiary customers in Nigeria. The case is under investigation by the Fiji Police Force.

3. In Indonesia's latest high-profile corruption verdict involving a tax collector, former Jakarta tax office director Bahasyim Assifie was convicted of corruption and money laundering related to bank accounts worth more than USD7 million in the names of his wife and children. He was sentenced to 10 years in prison.

   Part of the Indonesian FIU's Analyst Result, which was disseminated to the investigator, claimed that the Rp66 billion (USD7.3 million) in his accounts did not come from honest sources. Bahasyim's claims that he invested the money abroad and ran a jewellery business were not supported by convincing evidence, the judge said. His business partners in the Philippines and China had presented statements that they jointly ran several businesses with Bahasyim, but those statements were one-sided and prepared only after the case was prosecuted. It is believed that the defendant collected Rp60 billion plus USD681,000 between 2002 and 2009 through illegal means by misusing his position and authority as a civil servant. The judge said Bahasyim, in his official report to the Corruption Eradication Commission (KPK), claimed that his fortune was valued at only Rp10 billion.

   Investigations found that Bahasyim, 58, kept his money in bank accounts in the names of his wife, Sri Purwanti, and his daughters, Winda Arum Hapsari and Riandini Resanti. Winda, who had Rp17 billion in one of her accounts, was still a student when the accounts were opened. As a civil servant, the defendant normally received only Rp20 million to Rp30 million per month, the judge noted. In addition to the prison time, the panel also ordered the money in the family accounts to be seized by the state.

Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) found over 300 transactions involving the family accounts worth a total of around Rp932 billion (USD 93,624,117). Bahasyim regularly circulated the money among the various family accounts in transactions so numerous that they raised suspicion at INTRAC. Bahasyim also bought a house worth about Rp8 billion (USD803,640) in Jakarta's upscale Menteng district in 2005 and registered it under his son's name. The defendant said the money was meant as business loan to a company belonging to his son, Kurniawan Arifka. Bahasyim also failed to present evidence of a business agreement or other deal to support the claim that the money was meant as an investment, said the panel.

Bahasyim became director of tax examinations and investigations in the Jakarta tax office in October 2002, with the power to interrogate taxpayers, seize documents, launch searches and recommend legal action. He held several positions in the Jakarta Tax Office between 2002 and 2007, and was moved to the National Development Planning Agency (Bappenas) in 2008.

4. Mr X made transfers from Bank A to Bank B, amounting to over $6 million shortly after opening an account in Bank B. After such transfers, Mr X then used a third party as a nominee to buy/sell shares in overseas capital markets. Mr X got a significant gain by selling all the shares shortly after the share price sharply rose up. The same transaction pattern repeatedly happened in the following weeks. Mr X finally cashed out all the gains which were almost double from his investment capital.

   After the FIU's investigation, it was found that there were a lot of STRs related to these overseas listed companies. These companies had been abused for a long time as a puppet in the hands of speculators who had ties to the chairmen of these companies. The chairmen were being accused of market manipulation and insider trading.

5. A syndicate scammed victims into transferring their monies into third parties' accounts by making phone calls to the victims. The fraudster would claim to be and officer from the central bank or police headquarters or a commercial bank who was investigating the

victim's bank account for suspected irregular activities. For example, alleging that the victim's credit card has been abused for purchasing merchandise locally/abroad.

Victims were instructed not to hang up the phone while the fraudster transferred the call to supposedly the relevant investigation department officers. The technology used by scammers is called spoofing via Voice over Internet Protocol (VoIP) which enables the telephone number of the relevant authorities or banks to be displayed on the phone. As the victims were convinced that they were speaking to officers in the relevant authorities/banks, victim were then told to transfer money to a 3rd party account in the pretext of safeguarding the victim's money or to make payment to a special account pending investigations to avoid being charged in court.

Investigations revealed that the syndicate advertised in the local newspapers to target and recruit individuals comprising mainly youths/students/lower income job holders to create a pool of 3rd party savings accounts. The third party accounts were opened with a minimum deposit amount and were then used to receive the funds deposited by the victims shortly after the opening of the account. This was then followed by immediate withdrawals in cash within one (1) hour. Third party account holders were reported to receive between RM250 (USD76) to RM1,000 (USD306) plus commission for every account opened and when monies were successfully transferred by victims. The case is currently being investigated for cheating and money laundering offences.

6. Tan Wei Chong was a relationship manager with the Overseas Chinese Banking Corporation. Between October 2009 and August 2010, in the course of his work, he misappropriated customers' funds totalling USD4.72 million and EUR 88,122. The Commercial Affairs Department (CAD) investigation revealed that Tan Wei Chong withdrew monies from the accounts of four customers in 23 transactions.

   He submitted forged documents to his bank colleagues to deceive the bank into believing that the account holders were applying to transfer funds from their accounts. He used the same ruse to make eight cash withdrawals from the accounts. In these fraudulent transactions, he either used forms signed in blank by the account holders or simply forged their signatures on the documents. To avoid detection, Tan routed the monies taken from

the customers' accounts through bank accounts of his family members and he eventually withdrew the money in cash. All that money was spent on his gambling habit. Tan Wei Chong was betting excessively with internet casinos and soccer gaming sites.

On 1 June 2011, Tan Wei Chong was charged in court for 31 counts of cheating and 15 counts of money laundering. On 29 June 2011, he was sentenced to seven years' imprisonment after pleading guilty to 11 cheating charges and four money laundering charges.

7. FB is a former high-ranking officer of NN Bank's Wealth Management Group which catered to high value clients with bank deposits of less than Php4 million (USD92,724). FB allegedly lured clients into investing with him by promising higher interest rates for time deposits than what NN Bank offered and high referral fees over the standard rates. On 25 February 2011, NN Bank requested the FIU for an investigation and subsequent filing of a criminal complaint for money laundering against FB. According to NN Bank, FB, by virtue of his position of trust and confidence as Relationship Manager in NN Bank in its X Branch, embezzled at least USD14 million from his clients' accounts. FB simulated bank transactions in order to withdraw clients' funds without their knowledge and authorization. Thereafter, the funds were appropriated by FB and transferred to beneficiaries who had no connections at all to these clients.

   FB's fraudulent schemes were committed using the following means: (1) unauthorized funds transfer; (2) fictitious time deposit transactions; and (3) fictitious investment products allegedly purchased from FF Financial Services.

   Under the first scheme to defraud the depositors, FB caused the unauthorized fund transfers by withdrawing his clients' funds, or transferring such funds directly to his account or to the accounts of his beneficiaries or third parties. These withdrawals and fund transfers were made without the clients' consent or authorization, evidenced by the case withdrawal receipts with forged signatures and unauthorized applications for fund transfers.

   Under the second scheme, FB was able to obtain deposits from his clients by enticing them to invest in fictitious time deposit transactions. The database of NN Bank shows

that none of the purported time deposit confirmation forms were entered into the bank's system for processing; hence, these time deposits were fictitious and non-existent.

Under the third scheme, FB was able to entice customers to part with their funds by offering them fictitious investment products, such as fixed income investments, unit investment trust funds and registered mutual funds, allegedly offered by FF Financial Services. It was found that the documents, representing the investment products issued by FB to his customers, were falsified and non-existent based on the records of FF Financial Services.

Through these schemes, FB was able to defraud his depositors in eighty-two (82) transactions, with a total amount of Php97 million and USD832,000.

FB implemented the "hold mail" on all notices and statements and changed the registered mailing addresses without the client's knowledge or consent by replacing the same with the home address of a staff member, or his father's office, in order to prevent the client from receiving notices or statements which would reflect the fraudulent transactions.

FB tampered with some funds in order to utilize these unlawfully taken monies from the clients' accounts to run his National Basketball Association (NBA) cards trading business. Using these embezzled funds, he imported NBA cards from Country U through an entity named W Distribution and sold them through the internet to clients from Country U and Country R. FB used other persons and entities as beneficiaries of the stolen funds in order to run his NBA trading cards business and his money laundering activities. Funds that were obtained from clients' accounts were issued in the form of a manager's cheque, or were transferred to, or were the subject of fund transfers to, the accounts of:

His two partners, namely: EA of EA's Toy Car Shop, and Mr TA of TAE Collectibles. Mr SW, DG and W Distribution. SVG Development Inc. and SVG Corporate Holdings. PK, GE and RU. Mrs BCC, thru the latter's foreign exchange dealership; and OL and Ringside Inc. These persons and entities were consistently made the beneficiaries of the fraudulent transactions. W Distribution received as much as USD2.894 million.

Based on the FIU's investigation, it was confirmed that the dollar account of EA's Toy Shop with Account No. 444 in NN Bank was held jointly by EA and FB who both

opened the said account. There were fund transfers from this account to the account of SW and W Distribution. It was also found out that various movements/transfers of funds between the accounts of FB, SVG Development Inc., GE; PK and RU. FB, GE and PK and RU were among the shareholders of SVG Development Inc. and SVG Corporate Holdings. In 2009 and 2010, FB acquired three vehicles: Mercedes Benz C200 and E300 and Mazda CX-7. BCC was also the beneficiary of at least twenty-three (23) fraudulent transactions made by FB. An analysis of the database search showed that for every debit transaction/movement against the account of FB, a corresponding credit was also made on the account of BCC and/or Cano Mart.

Investigation reports also showed that FB processed at least forty-one (41) fraudulent transactions where OL and Ringside Inc. were the beneficiaries. In these transactions, FB, without authorization from his clients, purchased Manager's cheques from the accounts of two clients and deposited these cheques in the names of OL, Ringside Inc. and its directors JL and HS. The total amount of the fraudulent transactions is Php33.070 million (USD 766,574). Investigation by the FIU disclosed that FB held various accounts with FF Bank located in Country K. A petition for civil forfeiture has already been filed by the FIU against the funds that were generated by the frauds committed by FB and his cohorts.

VII. Gambling activities (casinos, horse racing, internet gambling etc.)

1. An Asian crime syndicate, which included an expert forgery artist, recruited foreign students to open bank accounts, steal mail and launder stolen cash. The students were among a number of third parties, also referred to as 'runners', enlisted to commit crimes for the syndicate.

   The scam began with the theft of cheques and credit cards from private mailboxes. The stolen documents were altered to create forgeries of sufficient quality to deceive bank tellers. The foreign students would deposit the cheques into their own bank accounts or accounts set up using false names. When a cheque cleared, the money was withdrawn and gambled at casinos to mix or co-mingle it with legitimate cash – a common money laundering methodology.

An investigation uncovered more than 350 falsely named bank accounts that had more than AUD8 million laundered through them. Suspicious matter reports (SMRs) submitted by banks indicated that one member of the syndicate had made regular deposits below the AUD10,000 threshold for reporting cash transactions to AUSTRAC.

One suspect was arrested and charged with eight counts of dealing with the proceeds of theft. The individual had allegedly stolen a cheque for more than AUD500,000 from a deceased estate. The individual attempted to launder the proceeds of the fraudulently obtained cheque through a casino. A second suspect was arrested and charged with six offences, including making a false document to obtain a financial advantage. A third suspect was also arrested and charged with identity fraud and money laundering offences.

Indicators in this case included:

- Customer making large cheque deposits despite having no known source of income.
- Customer undertaking transactions that appear inconsistent with their profile and transaction history.
- Large-value cheque deposits into newly opened, or student, bank accounts followed by immediate cash withdrawals once cleared.
- Structuring of cash deposits to avoid reporting requirements.
- Use of false identification to open bank accounts and conduct transactions.

VIII. Investment in capital markets, use of brokers

1. A law enforcement agency conducted an investigation into a suspect who operated a Ponzi scheme in which approximately 220 victims lost more than AUD15.5 million they believed had been invested legitimately. Over a nine-year period the suspect maintained a facade of heading a successful investment business. As the director of a group of companies, the suspect claimed to operate a legitimate managed investment scheme, including self-managed superannuation funds (SMSFs). The suspect claimed to trade in global derivatives and equity markets, promising extraordinarily high returns to potential investors. The scheme grew by word of mouth with friends, relatives and acquaintances

of the suspect and victims investing in the scheme. Victims of the scheme were from Australia, South Africa and the United Kingdom. While some victims initially received money from their investment, the majority lost their investments, including family inheritances, retirement funds and savings.

AUSTRAC information contributed to the investigation by identifying bank accounts, international funds transfer instructions (IFTIs) and transactions made by victims. AUSTRAC information identified bank accounts in Vanuatu linked to the suspect. Some victims reported signing contracts and transferring money to a company based in Vanuatu. AUSTRAC information indicated that money transferred to Vanuatu was later transferred to Australia, predominantly for the benefit of the suspect. All IFTIs linked to the scheme were made through banks and some incoming IFTIs represented transfers from overseas victims. AUSTRAC information showed that over a four-year period:

- Incoming IFTIs totalled more than AUD1.4 million, with the majority of the funds transferred from Vanuatu and New Zealand. IFTIs were also received from the United Kingdom.
- Outgoing IFTIs totalled more than AUD610,000, of which more than AUD500,000 was transferred to Vanuatu.
- Analysis of the transaction data showed most of the funds the suspect received from victims were applied for purposes other than investment. Of the AUD15.5 million received from victims, AUD6.6 million was returned to investors as either 'false returns' or as payments when investors left the scheme. More than AUD2.8 million was invested in high-risk derivative trading which returned only AUD900,000.
- More than AUD10 million was spent to support the suspect's lifestyle and pay for business expenses. Significant business expenses were outlaid to maintain the illusion of a successful managed investment scheme, including rent for a well-appointed office in a popular location.
- Subsequent analysis of financial data showed monthly transfers between AUD30,000 and AUD50,000 from the accounts of the group of investment companies to the suspect's credit card account. The suspect also raised more than

AUD36,000 in donations for two charities, which the suspect used for personal and investment purposes.

- The suspect was charged with seven offences relating to fraud and forgery, and was sentenced to 13 years imprisonment.

2. A foreigner, Mr Y, came to Macao SAR, China and setup an offshore investment company and opened a bank account under the company's name. Mr Y also setup a website to demonstrate the investment company's background and achievements for potential investors, stating that the company had a strong investment team that could help to invest in stocks with a high return in short period of time. Mr Y started reaching out to clients worldwide by phone and email to persuade them to invest funds in stocks. As a result, a number of clients around the world remitted funds amounting to over USD8 million to the investment company's bank account. After receipt of the funds, the balance was transferred out and the account was cancelled. As per the incident reported, and after investigation, two of the victims reported in person to claim and the suspect was identified. The case is still in the process of further litigation.

IX. Use of shell companies/corporations

1. AUSTRAC information assisted law enforcement to identify a criminal syndicate which was facilitating large-scale tax evasion for a number of clothing manufacturers. Investigations revealed that over a three-year period, more than AUD52 million was deposited into and withdrawn from accounts operated by the syndicate. Many of these transactions were reported to AUSTRAC by reporting entities via the submission of significant cash transaction reports (SCTRs). During this period the annual financial activity of the syndicate increased dramatically from approximately AUD750,000 in the first year to more than AUD17.5 million in the last year.

   The syndicate would receive cheques from the manufacturing businesses and deposit them into accounts linked to 'shell companies'. Once the cheques had cleared, the syndicate would withdraw the cash in multiple amounts and secretly return the cash to the

businesses. Two suspect transaction reports (SUSTRs) submitted by reporting entities triggered AUSTRAC's automated monitoring system. The information in the SUSTRs, along with AUSTRAC's additional analysis of related financial activity, identified 10 clothing manufacturing businesses in one geographic location which had been conducting large cash withdrawals over an extended period of time.

The SUSTRs also identified unusual financial activity involving members of the syndicate who were frequently depositing cheques into company accounts, followed by cash withdrawals equivalent in value to the cheque deposits, on the same day. This information prompted AUSTRAC to produce a financial intelligence assessment report for law enforcement agencies about these businesses. The fraud allowed the manufacturing companies to evade income tax and other taxation obligations and move their profits into the cash economy. Authorities believe that, because employees working for the manufacturing companies were paid in cash, they were also able to claim welfare benefits while working.

The method used by the syndicate to facilitate tax evasion is as follows:

- A number of legitimate clothing retail companies paid a clothing manufacturing company for the production of garments. These payments were for legitimate business activity and the retail companies were not complicit in the scheme.
- The promoters of the scheme made approaches to the garment makers and offered to help them to reduce the amount of tax they were paying, less payment of a commission to the promoters of between 5 per cent and 10 per cent.
- A series of shell companies were set up using details of members of the group of companies who had been approached by the promoters and paid a small amount of money for their personal details. These details were then used to register the companies, obtain workers compensation insurance and open bank accounts in order to create a facade of legitimacy.
- With the assistance of the promoters, the shell companies created false invoices and issued them to the clothing manufacturers for the provision of fictitious goods and services. These false invoices enabled the manufacturer to claim tax deductions for subcontracting expenses that were never incurred.

- The manufacturers made cheques payable to the shell companies to pay the false invoices.
- Members of the syndicate deposited the cheques into the accounts of the shell companies.
- Once the cheques had cleared, the syndicate members withdrew the funds from the accounts via multiple cash withdrawals using debit cards issued to the accounts of the shell companies. These withdrawals were undertaken across various bank branches.
- The syndicate returned the cash to the manufacturer, minus a commission.
- The manufacturers used the cash to fund their lifestyles and pay cash wages to their employees, thereby avoiding income tax obligations.

Further investigations revealed that a bank assistant manager had maintained a close relationship with the syndicate. The assistant manager used her influence over other bank staff to ensure AML/CTF reporting procedures were ignored. Members of the syndicate had also offered gifts to bank tellers to build rapport and encourage them to skip some stages of their AML/CTF program, thereby helping the syndicate avoid detection by AUSTRAC. Typically, a complicit staff member would allow a syndicate member to withdraw funds from multiple shell company accounts at the same time, even though they did not have the right to do so. The promoters actively sought the services of these bank staff, even knowing which staff would be working on particular days of the week. The good working relationship law enforcement had with members of the bank's AML/CTF team proved to be vital in the ultimate success of the law enforcement investigation. AUSTRAC also received a number of suspicious matter reports (SMRs) from reporting entities which helped reveal the methodology used by the syndicate. Within the SMRs, reporting entities identified the following 'grounds for suspicion':

- Several cheques written by the manufacturing companies were deposited (often several times in one day) by the syndicate members into multiple accounts operated by the shell companies. The syndicate members repeatedly requested quick clearances for the cheques.

- Funds were withdrawn from accounts as cash as soon as the proceeds of cheque deposits cleared, often on the same day, across multiple branches.
- The manufacturing businesses were associated with more than AUD16 million in cash withdrawals over a twelve-month period.
- When law enforcement officers moved to stop the syndicate, they restrained more than AUD1 million in cash, as well as a number of properties. Two members of the syndicate who facilitated the scheme were charged with dealing in proceeds of crime worth AUD1,000,000 or more.

Indicators involved in this case included –

- Customer offers incentives to representatives of a financial institution to assist bypassing AML/CTF procedures.
- Repeated requests for quick cheque clearances by customer.
- Same day cheque deposits, followed by cash withdrawals of an equivalent value to the cheque deposits, across multiple branches.
- Significant value and volume of cash withdrawals.
- Significant value and volume of cheque deposits into bank accounts.

2. Mr X from country C registered an investment company and opened several multiple currency bank accounts in country M. Shortly after the accounts were opened, large amount of funds were transferred into the bank accounts through different channels, including cash, cheques, account transfers and remittances. Upon receiving the funds, Mr X immediately remitted them to different individuals and companies. Mr X claimed that the source of funds was investment funds from customers to invest in foreign property and the outflow was their dividends, most of the counterparts came from country C. Along the process, Mr X also set up several related companies in different parts of the world, and his partners and he held several property investment companies in country M with the same address. It was suspected that these related companies were shell companies. The transaction pattern was deemed unusual as the outflow of funds was made to other counterparts instead of the investors themselves, which did not correspond to the reason given of dividend distribution. In addition, the bank in country M also

revealed that the Mr X's partners opened several bank accounts with the same transaction pattern as Mr X.

With this case, the FIUs of these countries exchanged information for analysis and further investigation. It was revealed that most of the companies held by Mr X and his partners were shell companies, which might be involved in boiler-room operations or fraud cases overseas, and the bank accounts in country M were being used to transfer funds to overseas accounts.

3. X, a director of Company A, submitted fictitious invoices to a bank to induce the said bank to disburse six sums totalling about USD870,000 to X's sole-proprietorship (Business B). These sums were purportedly to pay a foreign company for purchases, financed by Company A's trade credit facilities with the bank. After receiving the monies from the bank, Business B transferred about USD 155,000 to X's personal account in Singapore. Another USD700,000 was transferred to a Channel Islands private bank account maintained by a shell company (Company C) registered in the British Virgin Islands. X and his wife were the directors of Company C. About USD615,000 was subsequently transferred from Company C's Channel Islands bank account to X's personal account in Singapore. Most of the criminal proceeds consolidated in X's personal account were subsequently used to purchase two properties in Singapore. Some of the proceeds were also used to purchase mobile phones and jewellery.

   X was eventually prosecuted on four Money Laundering charges, of which two were related to removal of criminal proceeds out of Singapore, one related to conversion of criminal proceeds into property and one related to transferring of criminal proceeds. The Court sentenced X to 15 months imprisonment for money laundering. The sentence was to run concurrently with X's predicate offence sentence of 54 months imprisonment.

X. Use of the internet (encryption, access to IDs, international banking, etc.)

1. AUSTRAC alerted law enforcement authorities to frauds facilitated by a suspect in Australia who was part of a large-scale Nigerian fraud network. The suspect allegedly scammed more than AUD500,000 from overseas victims via the internet.

   The suspect came to AUSTRAC's attention after a suspect transaction report (SUSTR) was submitted by a reporting entity. The report, which had triggered AUSTRAC's automated monitoring system, revealed that the suspect had conducted unusually high-volume and high-frequency international funds transfer instructions (IFTIs) to Nigeria. The funds transfers were paid for in cash and appeared to be structured to avoid the threshold transaction reporting requirements. Authorities established that the suspect used variations of her name when conducting transactions. AUSTRAC staff analysed financial transaction reports submitted by reporting entities and identified the following:

   - Over a 10-month period the suspect undertook 35 outgoing IFTIs totalling approximately AUD160,000. The funds were consistently sent to two recipients in Nigeria.
   - International funds transfers were conducted through a remittance service provider and paid for with cash. The cash payments were seemingly structured into amounts of less than AUD10,000 to avoid the cash transaction reporting threshold.
   - Over a 10-month period the suspect was the recipient of nine incoming IFTIs from the United States totalling approximately AUD140,000, suspected to be the proceeds of the fraud.
   - The suspect conducted numerous large cash withdrawals and deposits which were detailed in significant cash transaction reports (SCTRs) submitted to AUSTRAC. Over a two-month period the suspect withdrew cash totalling more than AUD86,000 and deposited cash totalling more than AUD52,000.
   - Over an 11-month period, reporting entities submitted seven SUSTRs to AUSTRAC about the suspicious activities of the suspect. The SUSTRs identified unusually large cash transactions to fund IFTIs to Nigeria and the apparent structuring of transfers to avoid the cash threshold reporting requirements.

AUSTRAC identified that the funds sent to Nigeria appeared to be sourced from a number of cash withdrawals made from the suspect's account and from funds sent from an individual in the United States directly to the suspect. A portion of the funds remained in the suspect's bank account and were believed to represent a commission. The resulting law enforcement investigation revealed the suspect operated the fraud from home and used various names to communicate with victims over the internet. The suspect secured payments from victims by asking for financial help. AUSTRAC searches were conducted on additional name variations the suspect used to perpetrate the scam. AUSTRAC information showed the suspect was the subject of an additional eight SUSTRs. Reporting entity staff observed that:

- within one month of opening a bank account, the suspect received approximately AUD150,000 and withdraw all the funds;
- the suspect's income and occupation were inconsistent with the high value of transactions she was undertaking;
- the suspect became evasive and upset when asked routine questions about a transaction requiring the submission of a SCTR; and
- the suspect changed the method of withdrawing funds seemingly to avoid threshold reporting requirements, by withdrawing the daily limit of AUD3,000 on a daily basis at various bank branches, then withdrawing another AUD1,000 from automatic teller machines (ATMs).

Further searches were conducted on name variations used by the suspect and identified that the suspect:

- received an additional AUD318,000 in incoming IFTIs from the United States and Canada;
- sent an additional AUD207,000 to beneficiaries in Nigeria, the United States, United Kingdom and Morocco;
- was the subject of an additional eight SCTRs for deposits totalling approximately AUD124,000 and 11 SCTRs for cash withdrawals totalling approximately AUD172,000; and
- may have provided false identification to conduct outgoing IFTIs to Nigeria.

Law enforcement officers executed a search warrant on the suspect's premises and seized cash totalling approximately AUD29,000. The suspect was arrested and charged with six counts of fraud and one count of possessing tainted property. The suspect was convicted and sentenced to six years imprisonment.

Indicators in this case:

- Cash withdrawals conducted at various bank branches and ATMs on the same day.
- Customer undertaking transactions which appear to be inconsistent with their profile and/or transaction history.
- High-value cash deposits to pay for international funds transfers.
- High-value international funds transfer to/from Australia for no apparent logical reason.
- Multiple high-value international funds transfer to a high-risk jurisdiction.
- Structured cash payments just below the cash reporting threshold used to pay for international funds transfers.
- Use of false identification to conduct transactions.

2. Person A was an unemployed businessman from Vanuatu and a resident in Fiji. Person B contacted him by email and phone and suggested a "business/investment arrangement". Person A acceded to this and gave his bank account to Person B. Person B was to remit US$15,000,000 to Person A to invest for him. However the funds were locked in the Bank of America and could only be unfrozen and remitted to the Person A on the payment of taxes to the bank. The money to pay these taxes would be credited to Person A's account by Person B and they were then to be sent on to a lady in Washington State, U.S.A. who work for the Bank of America to settle the outstanding taxes. Person A received two funds transfers into his account which he sent on to the lady as instructed. Most of the remittances were made through a foreign exchange dealer. Person A's account was credited with funds by telegraphic transfer from the Cook Islands. The funds credited/transferred to Person A's account were made through authorised access into some local customers bank account who fell victim to a phishing scam. Person A was

convicted and sentenced on 12 April 2012. He was charged for two counts of Money Laundering and sentenced to seven years imprisonment.

XI. Currency exchanges/cash conversion

1. The Indonesian FIU received Suspicious Transactions from a currency exchange dealer regarding Foreign Exchange on Forex USD exchange carried out by a Politically Exposed Person (Mr X) who conducted two transactions during April to May 2012 with a total value equivalent to Rp. 1.3 billion (USD30 million).

   Details of the transaction are as follows:

   At the time of the currency exchange, currency exchange cash proceeds are requested by Mr X to be directly transferred to the account of Property Company (PT R Develop Realty) amounting to Rp. 950 million and PT. X Mobilindo of Rp. 280 million. Having been traced at Bank X, it is known that the remittance transaction to the account of PT. X Mobilindo is a payment transaction on the purchase of an automobile for Son of Mr X, while the other remittance to the account of PT R. Develop Realty is a payment transaction on the purchase of apartment for Wife of Mr X. There is a tendency for disguising financial transactions in the purchase of valuable possessions using currency exchange transactions.

XII. Use of credit cards, cheques, promissory notes, etc.

1. Local commercial bank “B” filed an STR on the suspicion that the personal account of the president of a charitable organization was being credited with large sums of money. Investigations into the alleged transactions revealed that donations were made to the charitable organization using credit cards through the internet payment gateway provided by bank “B”. Once the funds were credited to the account of the charitable organization the funds were being transferred to various individual accounts including the account of its president and Treasurer. It was further revealed that the payment through credit cards had been made without the knowledge of the card holder, hence payments made through

the internet payment gateway had been charged back, incurring a loss of LKR 263 million (USD2 million) to the bank.

XIII. Wire transfers

1. Mr Han was the Chairman of Yang X Travel Agency. Mr Li was the manager of the agency's tourism department. In July 2009, the travel agency organized international group tours and collected a total of NTD5,736,884 (about USD200,000) from customers to cover the tour costs. The money was not used to pay tour expenses; instead it was appropriated for other purposes. As a result, the tours could not go ahead as scheduled. To prevent the capital from being confiscated after the agency's cheque bounced, Mr Han instructed Mr Li to wire over USD100,000 to Mr Li's personal account in the Cheng Dong Branch of First Bank, but purportedly for the Da X Travel Agency in Singapore to conceal it. Then, Mr Li used part of the money to pay off money owed to the tour groups and took the remaining NTD2,132,676 (about USD71,000) into his personal possession as salary and pension owed to him by the company. The case was referred to Taipei District Prosecutor's Office on May 20, 2011 by the Investigation Bureau.

2. A syndicate in jurisdiction A established two offshore trading companies and opened two bank accounts in Hong Kong. Between 2005 and 2008, numerous victims all over the world were deceived into remitting money (totalling about USD30million) into these two bank accounts. Acting on information provided by overseas LEAs, Police arrested two persons-in-charge of the companies, who were found engaging some remittance agents to remit the 'sales proceeds' via Hong Kong back to Jurisdiction A. The arrested persons were charged for Money Laundering offence(s) in Hong Kong.

XIV. Use of foreign bank accounts

1. T incorporated two companies in the British Virgin Islands and set up bank accounts for the two companies with banks in Singapore and another Asian Country. All the accounts

set up in Singapore could be operated via the internet. These accounts in Singapore were used to receive criminal proceeds from scam victims overseas. The perpetrators of the scam sent out emails in the name of an organization in Europe. The perpetrators informed the clients of the organization that they still owed the organization monies for the services rendered, and requested the clients to send the monies to one of the said accounts in Singapore. Monies received in the Singapore accounts were remitted out to bank accounts overseas within days of receipt. Within four months, more that USD 2 million passed through the accounts. T claimed that it was his friend, S, who approached him to conduct these acts and that all the instruments for the control of the accounts were handed to S. T claimed that he received USD20,000 for his work. T was eventually prosecuted for two ML charges relating to the facilitation of the transfers of criminal proceeds. There was no evidence that he was involved in the predicate offence. The court convicted and sentenced T to 8 months imprisonment for money laundering.

12. USEFUL WEBSITES

- Financial Intelligence Unit- India — http://www.fiuindia.gov.in/
- FIInet Gateway — https://finnet.gov.in/
- Directorate of Enforcement — http://www.directorateofenforcement.gov.in/
- Ministry of Finance — http://www.finmin.nic.in/
- The Central Economic Intelligence Bureau — http://www.ceib.nic.in/
- Insurance Regulatory and Development Authority — http://www.irdaindia.org/
- Reserve Bank of India — http://www.rbi.org.in/
- Securities and Exchange Board of India — http://www.sebi.gov.in/
- Financial Action Task Force on Money Laundering (FATF) — http://www.fatf-gafi.org
- Asia/Pacific Group on Money Laundering (APG) — http://www.apgml.org/
- Caribbean Financial Action Task Force on Money Laundering (CFATF) — http://www.cfatf.org/eng/
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) — http://www.esaamlg.org/
- Egmont group — http://www.egmontgroup.org/
- Eurasian Group on Combating Money Laundering and Financing Terrorism — http://www.eurasiangroup.org/
- Middle East & North Africa Financial Action Task Force (MENAFATF) — http://www.menafatf.org/
- International Money Laundering Information Network (IMoLIN) — http://www.imolin.org/imolin/index.html

PROFESSIONAL OPPORTUNITIES

1. Drafting of KYC policy for Banks, insurance co and market intermediary
2. Drafting of AML policy
3. KYC Audit
4. FEMA compliance Audit
5. Appearing before appellate authority
6. Corporate Advisory
7. Framing Risk Management Policy

13. ANNEXURE

a. **RBI Master Circular KYC norms/AML standards (Banks), 2013**

b. **KYC Norms and AML standards – Guidance Notes for Banks – issued by Indian Banks' Association**

c. **RBI Master Circular KYC guidelines/AML standards (NBFCs), 2013**

d. **SEBI Master Circular AML/CFT obligations of Securities Market Intermediaries, 2010**

e. **SEBI {(KYC (Know Your Client) Registration Agency} Regulations, 2011**

f. **SEBI Guidelines in pursuance of the SEBI KYC Registration Agency (KRA) Regulations, 2011 and for In-Person Verification (IPV)**

g. **IRDA Master circular AML/CFT – guidelines for insurers**

h. **IRDA AML/CFT guidelines for general insurers**

i. **Master Circular - Anti Money Laundering/Counter-Financing of Terrorism (AML/CFT) – Guidelines for Postal schemes**