Chapter III: An overview of AML regimes and consequences of Laws on AML in the developed and developing countries

3.1 General

This part of research gives an overview of the general information on the U.K and U.S as developed and also India and Iran as DGCs and discusses about their economy, system of government, legal system and hierarchy of laws, situation of money laundering and anti-money laundering legislation.

U.K

The United Kingdom of Great Britain and Northern Ireland is a political union made up of four constituent countries: England, Scotland, and Wales on the island of Great Britain, and Northern Ireland. Estimates in mid-2008 indicated a population of 61,383,000. UK’s overall population density is one of the highest in the world. About a quarter of the population lives in England's prosperous southeast and is predominantly urban and suburban, with about 7.2 million in the capital, London. The literacy rate is 99% (as of 2008).

Figure 3.1 Map of U.K
U.S.

The United States of America (U.S.) is comprised of 50 states and one district. The U.S. covers an area of 9.6 million square kilometers, shares borders with Canada to the north and Mexico to the south, and is flanked by the Atlantic Ocean to the east and the Pacific Ocean to the west. The capital of the U.S. is Washington, District of Columbia (DC). As of 2005, the estimated population is 295,734,134 having a mean age of 36 and life expectancy averaging 77.7 years. The official language is English and the literacy rate is 99% (as of 2010).

Figure 3.2 Map of U.S
India

India is the largest democracy in the world, the seventh largest country and the second most populous. India has the world’s second largest population, estimated at 1.15 billion in 2008 (Sarina, 2009). India is located in south Asia and is often called a subcontinent. The Himalayan ranges crown the northern boundary of India. India is bounded on the north by Afghanistan, China, Nepal, and Bhutan; on the east by Bangladesh, Myanmar, and the Bay of Bengal; on the south by the Palk Strait and the Gulf of Mannar and the Indian Ocean; and on the west by the Arabian Sea and Pakistan. India is divided into 28 states and 7 Union Territories. New Delhi is the capital of India and one of its largest cities. The literacy rate in India is 65.38% (Sarina, 2009).

Figure 3.3 Map of India
Iran

Iran (officially The Islamic Republic of Iran) is located at the strategic crossroads between the Western and Eastern worlds. Iran has the second largest population (75 million people), after Egypt, in the Middle East and North Africa region. Covering a surface area of 1,648,195 square kilometers, it is bordered by Iraq on the west, Turkey on the northwest, the Republics of Armenia, Azerbaijan, Turkmenistan, as well as the Caspian Sea on the north, Afghanistan on the east, Pakistan on the southeast, the Persian Gulf and the Sea of Oman on the south. The Persian Gulf is the shallow marginal part of the Indian Ocean that lies between the Arabian Peninsula and the southwest Iran. The official language is Persian and the literacy rate is 84% (as of 2006).

Figure 3.4  Map of Iran
3.1.1 Economy

U.K

Based on market exchange rates, the UK is the fifth-largest economy in the world, the second largest in Europe after Germany, and the sixth-largest overall by purchasing power parity exchange rates. The currency of the UK is pound sterling, represented by the symbol “£”. The Bank of England is the central bank and is responsible for issuing currency, although banks in Scotland and Northern Ireland retain the right to issue their own notes, subject to retaining enough Bank of England notes in reserve to cover the issue. Since 1997, the Bank of England has exercised control of interest rates and other monetary policy, independent of Government. Government intervention in the economy is exercised at a macroeconomic level, primarily through HM Treasury, the UK’s economics and finance ministry (K. Holden, 1995).

U.S

The U.S. is a developed, industrial country with a free-market economy. The U.S. is the largest economy in the world with GDP valued in 2004 at USD 11.75 trillion, broken up into the service (79.4%), industry (19.7%) and agricultural (0.9%) sectors.

India

The economy of India is the fourth largest in the world, with a GDP of $3 trillion (2007) when measured on purchasing power parity (PPP) basis. India’s Economy has grown by more than 8.8% for five years running, and has seen a decade of 7.2%+ growth (Saumitra, 2009). This has reduced poverty by 10%, but with 60% of India’s 1.1 billion populations living off agriculture and with droughts and floods increasing, poverty alleviation is still a major challenge. The Rupee is Indian’s official currency.

Iran

According to The World Bank Report (September 2008), Iran has a mixed economy that is heavily dependent on export earnings from the country's extensive petroleum reserves. Iran is OPEC's second largest oil producer, as it exports 3.3 million (2003 estimate) barrels of oil per day; moreover, it holds 10% of the world's confirmed oil reserves. Iran also has the world's second largest natural gas reserves (after
Russia. Oil exports account for nearly 80 percent of foreign exchange earnings. In July, 2006, the Government announced a major privatization program whereby large, strategic industries mandated to be state-owned by Article 44 of the Constitution could be privatized. These include, among others, the downstream oil sector, the utilities sector, a large proportion of the financial sector, and the large industrial and commercial sectors. However, implementation of the program has been hindered by low demand for large public sector assets by the private sector. Iran's gross national product (GNP) is the highest in the Middle East, although its GNP per capita is comparatively low because of Iran's large and growing population.

"Bank Markazi Jomhouri Islami Iran" is the central bank of the Islamic Republic of Iran. The Central Bank of Iran (CBI) is responsible for the design and implementation of the monetary and credit policies with due regard to the general economic policy of the country. The Iranian rial (IRR) is Iran’s official currency.

3.1.2. System of government

U.K

The UK is a constitutional monarchy, with executive power exercised on behalf of Her Majesty Queen Elizabeth II by a democratically elected Prime Minister and other "Cabinet Ministers" who head the departments of state. The UK does not have a codified constitution, relying instead on traditional customs and separate pieces of constitutional law. While the Queen is Head of State and theoretically holds all executive power, the Prime Minister is the Head of Government. The Parliament, the legislative body, is traditionally considered to be “supreme” (that is, able to legislate on any matter and not bound by decisions of its predecessors). Parliament consists of one entirely elected chamber, the House of Commons, and one part-hereditary part-appointed chamber, the House of Lords. An Act of Parliament does not become law until it has been signed by the monarch ("royal assent"). The party that commands a majority in the House of Commons further to a General Election (held once every 4-5 years) is normally appointed as Her Majesty’s Government - or, if there is no majority party, the largest coalition.
U.S

The U.S. is a constitution-based federal republic with executive, legislative, and judicial branches. The executive branch comprises an elected President and Vice-President, and an appointed Cabinet. The federal legislative branch, known as Congress, consists of a House of Representatives (containing 435 members, with each state’s number of representatives commensurate with its population) and the Senate (containing 100 members—two per state). The judicial branch is made up of the U.S. Supreme Court, Federal Courts of Appeal, and Federal District Courts. There are also courts on the state level, including state-wide and local county-level courts (FATF, 2006).

India

India, a union of states, is a Sovereign Socialist Secular Democratic Republic with a Parliamentary system of Government. Sovereignty is shared between the central government and the states, but the national government is given greater powers. The President is the constitutional head of Executive of the Union. Real executive power vests in a Council of Ministers with the Prime Minister as head. The Council of Ministers headed by the Prime Minister to aid and advises the President who shall, in exercise of his functions, act in accordance with such advice.

The Council of Ministers is collectively responsible to the Lok Sabha, the House of the People. The State government resembles the federal system. In the states, the Governor is the head of Executive, but real executive power vests with the Chief Minister who heads the Council of Ministers. The Council of Ministers of a state is collectively responsible to the elected legislative assembly of the state. The governor of each state is appointed by the President. The central government exerts greater control over the union territories than over the states, although some territories have gained more power to administer their own affairs.
Iran

Iran is an Islamic Republic established following the Islamic Revolution of 1979. Under the Constitution of Nov 1979 all cultural, social, political, and economic institutions of Iranian society are to be based on the Islamic principles and norms. All government policies are supervised and correlated with Divine decrees through the Vali-e Faqih (Jurisconsult or the Supreme Leader). According to the constitution he is responsible for this concordance before God and the people during the time when the 12th Imam is in occultation. The country is divided into 31 Ostans (provinces) ruled over by an Ostandar (governor-general).

3.1.3 Legal system and hierarchy of laws

U.K

The Parliament at Westminster remains the seat of Government for the UK, Scotland, Wales, and Northern Ireland have a degree of devolved government. This is exercised through, respectively: the Scottish Parliament, the National Assembly for Wales, and the Northern Ireland Assembly. The Scottish Parliament of 129 members is elected every four years. It operates broadly on the Westminster model, electing a First Minister who heads the “Scottish Executive.” The National Assembly for Wales has 60 members. It does not have the power to make primary legislation, but enjoys extensive executive powers and may make secondary legislation. The Northern Ireland Assembly consists of 108 members with a similar range of legislative and executive powers to the Scottish Parliament.

The U.K has three distinct jurisdictions: Scotland, Northern Ireland, and England and Wales which for legal purposes counts as a single jurisdiction. England and Wales and Northern Ireland are common law jurisdictions, whereas Scotland operates a hybrid system based on both common law and civil law principles (Slapper& Gary, 2001).
U.S

In the U.S each state has its own unique legal system, of which all but one (Louisiana) is based on common law. The U.S. Constitution enumerates the broad areas where the federal government has legislative authority. Some powers are exclusively federal because the constitution limits or prohibits the use of the power by states or because the nature of the power itself is such that it can be exercised only by the federal government (Financial Action Task Force, 2006).

Regulations are promulgated in accordance with the practices and procedures set out in the Administrative Procedure Act (APA). Among other requirements, the APA generally requires all government agencies with powers to administer federal laws to give public notice and solicit public comment on substantive rules of general applicability adopted as authorized by law.

A self implementing statute is enforceable on and after its effective date. Some laws, however, require implementing regulations to give them effect and are not fully enforceable until such implementing regulations have been issued. Implementing regulations adopted pursuant to a law are fully enforceable once they have been properly promulgated in accordance with the procedure set out below and on the published effective date.

In general, the agency that is undertaking to promulgate a new regulation publishes a “notice of proposed rulemaking” (NPRM) in the Federal Register (FR), and specifically seeks public comment on its proposed action within a prescribed time frame. Such a notice includes the legal authority for the agency’s issuance of the rule, proposed regulatory language (the “proposed rule”), and a full discussion of the justification and analysis behind the rule. Proposed rules have no force and effect. After the close of the comment period, the promulgating agency considers all comments timely submitted in response to the notice of proposed rulemaking. The agency may then adopt and publish a “final rule” which provides notice to the public of the text of the rule as adopted, a summary and analysis of comments received and the rationale for adopting the rule in the form published. In general, a final rule does not become effective immediately, but rather specifies an effective date, usually 30 days after publication of the final rule in the Federal Register. A final rule becomes
effective following publication, on its effective date. If after publishing the notice of proposed rulemaking the agency feels there are certain issues upon which it wishes to receive additional comments, the agency may take various steps to continue to solicit additional comments, before issuing a final rule, including the issuance of an “interim final rule” (IFR). An IFR is enforceable as a final rule upon its effective date. After receiving additional public input, the agency may then publish a final rule. The IFR remains in effect until superseded by the issuance of a subsequent final rule (Financial Action Task Force, 2006).

**India**

India has a bicameral parliament including the Rajya Sabha (Council of States) and the Lok Sabha (House of the People). The members of Lok Sabha are elected directly by all eligible voters and sits for 5 years unless dissolved earlier. The legislatures of the states and union territories elect 233 members to the Rajya Sabha, and the president appoints another 12. The elected members of the Rajya Sabha serve 6-year terms, with one-third up for election every 2 years. The Lok Sabha consists of 545 members; 543 are directly elected to 5-year terms. The other two are appointed. National and state elections are ordinarily held every five years, although they may be postponed in an emergency and may be held more frequently if the government loses a confidence vote. The main function of both the Houses is to pass laws. Every Bill has to be passed by both the Houses and assented to by the President before it becomes law.

**Iran**

In Iran the legislative wing of the State, Majlis-e Shura-ye Eslami (Islamic Consultative Assembly) consists of 270 representatives elected by the direct vote of the people for a term of four years. The Constitution has also provided for a constitutional council of sages known as the Council of the Guardians of the Constitution (Shura-ye Negahban-e Qanun-e Assasi) which has the power to either approve or vote out the Assembly's resolutions. The Assembly of Experts (Majlis-e Khebregan), is another Islamic body responsible for the choosing of a Leader in the event of the present leader's demise, or to replace him with another one if required.
3.1.4 Situation of Money laundering

U.K

According to Vickers (2005) Billions of ‘dirty’ pounds are mistakenly ‘cleaned’ by Financial Institutions and professional advisers, or received by businesses turning a blind eye to large cash payments. As a consequence, money laundering represents a serious threat, not just to sound economic and financial development but to the political integrity and stability of our nation.

The NCIS ‘United Kingdom Threat Assessment of Serious and Organized Crime’ in 2003 stated that the overall size of criminal proceeds in the country – and the amount that is laundered is unknown. However, customs authorities had estimated that the annual proceeds from crime in the UK were anywhere between £19 billion and £48 billion – with £25 billion being a realistic Graph for the amount that is laundered each year (lilley, 2006).

UK law enforcement estimates the economic and social costs of serious organized crime, including the costs of combating it, at upwards of £20 billion a year. It is estimated that the total quantified organized crime market in the UK is worth about £15 billion per year as follows: drugs (50%); excise fraud (25%); fraud (12%); counterfeiting (7%); organized immigration crime (6%). Estimated total recoverable criminal assets per annum are £4.75 billion, of which it is estimated that £2.75 billion is sent overseas.

U.S

According to U.S. Money Laundering Threat Assessment (2005), proceeds from the sale of illicit narcotics are a major source of demand for money laundering in the U.S. The most prevalent method of money laundering reported in suspicious activity reports (SAR) is structured cash deposits followed by immediate and regular international wire transfers that are conducted through correspondent accounts either by individuals or businesses. Other methods include the use of bulk-cash smuggling, trade-based money laundering, insurance products, casinos and MSBs, including informal value transfer services (IVTS) to transmit illicit proceeds. Since the implementation of stricter customer due diligence and recordkeeping requirements,
the IRS-Criminal Investigation (IRS-CI) has noted that Financial Institutions are used to a lesser extent to facilitate money laundering. Techniques and trends that continue to be observed by law enforcement agencies can be summarized as follows.

**Banking sector:** According to James Petras (2001), an incomplete Graph of dirty money (laundered criminal and corrupt money) flowing into the U.S. coffers during the 1990s amounted to $3-$5.5 trillion. There is a consensus among U.S. Congressional Investigators, former bankers and international banking experts that U.S. and European banks launder between $500 billion and $1 trillion of dirty money each year, half of which is laundered by U.S. banks alone. According to Senator Carl Levin, “Estimates are that $500 billion to $1 trillion of international criminal proceeds are moved internationally and deposited into bank accounts annually”. It is estimated that half of that money comes to the United States).

**Insurance sector:** According to U.S. Money Laundering Threat Assessment (2005), Life, health, and accident insurance generate more than half a trillion dollars in premiums and contract revenue annually for U.S. insurers. Money laundering through insurance has been generally confined to life insurance and annuity products. The inclusion of investment products with the usual portfolio of insurance policies has increased the potential for insurance companies to be used as ML conduits.

**Money Orders:** Money orders are a highly versatile vehicle for money laundering, useful for a number of financial crimes ranging from smuggling narcotics trafficking proceeds to depositing illicit proceeds from alien smuggling and corporate fraud into bank accounts. Money orders are used by approximately 30 million people annually to conduct business such as paying bills and sending money back to families in foreign countries. It is estimated that over 830 million money orders in excess of $100 billion are issued annually (U.S. Money Laundering Threat Assessment (2005)).

**Foreign Trade Zones (FTZs):** Foreign Trade Zones (known as Free Trade Zones outside of the United States are intended to promote manufacturing in the host country, but can also be used to facilitate money laundering. Often, criminal operations within an FTZ involve some type of import/export scheme. False documentation involving fabricated Bills of Lading and fictitious names and addresses are used to misrepresent imports and exports, often with a customs broker.
who is in collusion with the criminals, “brokering” the documents with CBP (U.S. Money Laundering Threat Assessment, 2005).

**Bulk cash smuggling:** From 2001 through February, 2005 Immigration and Customs Enforcement (ICE) agents arrested more than 260 individuals for bulk cash smuggling violations. Approximately 20% of the arrests resulted from seizures not at a border or port of entry, but in the interior of the United States. In addition, ICE and Customs and Border Protection (CBP) have seized a combined total of more than $107 million in cases where bulk cash smuggling was charged (U.S. Money Laundering Threat Assessment, 2005).

**Trade-based money laundering:** According to U.S. Money Laundering Threat Assessment (2005), Trade-based money laundering encompasses a variety of schemes that enable the cash to be separated from the crime early in the money laundering process. The BMPE is responsible for moving an estimated USD 5 billion worth of drug proceeds per year from the U.S. back to Colombia.

**Shell companies:** Fin CEN reports that 397 SARs (representing an aggregate of USD 4 billion) were filed between April, 1996 and January, 2004 involving shell companies, and the use of foreign correspondent bank accounts.

**Informal Value Transfer Systems:** (IVTS) are efficient remittance systems based on trust that operate primarily within ethnic communities. Since the enactment of § 1960, ICE has initiated more than 260 IVTS investigations and executed more than 100 search warrants in connection with these cases. During this period, ICE investigations into unlicensed MSBs have resulted in roughly 120 arrests, 130 indictments, and the seizure of some $23 million (U.S. Money Laundering Threat Assessment, 2005).

**Casinos:** Based on U.S. Money Laundering Threat Assessment (2005), More than $800 billion was wagered at approximately 845 casinos and card clubs in the United States in 2003, accounting for approximately 85 percent of the total amount of money wagered for all legal gaming activities throughout the country.
India

According to International Narcotics Control Strategy Report (2007), India has illegal black market channels for selling goods. Smuggled goods such as food items, computer parts, cellular phones, gold, and a wide range of imported consumer goods are routinely sold through the black market. By dealing in cash transactions and avoiding customs duties and taxes, black market merchants offer better prices than those offered by regulated merchants. However, due to trade liberalization and an increase in the number of foreign companies doing business in India, the business volume in smuggled goods has fallen significantly. Most products previously sold in the black market are now traded through lawful channels. In India, Kaldor’s estimates for black money generation in 1953-54 were about Rs. 600 crores (i.e. 6% of National Income then) on account of tax evasion only. Some of the other estimates further have been Rs. 700 crores (1961-62); Rs. 1,000 crores (1965-66); Rs. 1,400 crores (1968-69). Other estimates by Dr. Rangnekkar for the same periods were Rs. 1,150 cr, Rs. 2,350 crores and Rs. 2833 crores respectively. The Indian Institute of Finance (IIF) study indicated that the growth rate of black money in 1991 has been at a rate of Rs. 60,000 crores per year (Agarwal, 1991). Black money generated from legal activities accounts for the parallel economy in India, which is considered to be as strong as the normal economy. It is estimated that the yearly growth rate of Black money is a factor to the tune of 40-50% of GDP growth in the Indian economy on a year to year basis (Vittal, 2002).

According to the Annual Report of the United Nations, Asia and Far East Institute (2000), Money laundering techniques include smuggling, establishment of front companies, acquisition of commercial and non commercial properties, remittances through Hawala or Hundi. Over invoicing and double invoicing of goods through foreign remittances and through trading in stock and shares. The Indian “Hawala” or “Hundi” system of transaction can be explained as transfer of money through unofficial and non banking channels. The money so transferred often includes the money derived from criminal activities in violation of the country’s legislation.

According to International Narcotics Control Strategy Report (2007), the Hawala market is estimated at anywhere between 30 and 40 percent of the formal market.
Remittances to India reported through legal, formal channels in 2005-2006 amounted to $24 billion (reportedly the largest in the world).

**Iran**

According to International Narcotics Control Strategy Report (2007), in Iran organized criminal activities and money laundering pose a major challenge to the society. Reportedly, a prominent Iranian banking official estimates that money laundering encompasses an estimated 20 percent of Iran's economy. There are other reports that over $11 billion a year is laundered via smuggling commodities in Iran and over $6 billion is laundered by international criminal networks. The World Bank reports that about 19 percent of Iran's GDP pertains to unofficial economic activities. Money laundering in Iran encompasses narcotics trafficking, smuggling, trade fraud, counterfeit merchandise and intellectual property rights violations, cigarette smuggling, trafficking in persons, Hawala, capital flight, and tax evasion.

3.1.5 Anti-Money Laundering Legislation

**U.K**

In the UK there are principally four sources of authority with regard to money laundering, the primary legislation, the Money Laundering Regulations (Statutory Instruments), the Financial Services Authority (FSA) Rules and the Joint Money Laundering Steering Group (JMLSG) Guidance Notes (industry guidance) (Raphael, 2006). The relationship between these four sources of authority can be summarized as figure 3.5.
The U.K has had specific legislation against laundering the proceeds of drug trafficking since the Drug Trafficking Offences Act (DTOA) 1986. Since then more legislation has been enacted and primary legislation now covers the laundering of proceeds from drug trafficking, terrorism and general crime. However, the legislation has not yet been consolidated and important differences remain between treatments of these three types of proceeds.

The following Acts of Parliament not only contain provisions against money laundering, but they also form a chronology of the developments in the battle against it in the UK (Billy Steel, 2010).

- **Drug Trafficking Offences Act 1986 (DTOA):** This is significant in fighting the drugs money threat. Has now been mostly repealed and the money laundering laws relating to drugs trafficking moved to the DTA94.

- **Criminal Justice (Scotland) Act 1987 (CJSA):** This is now repealed, this set up the first confiscation mechanism in Scots Law (Section1).
B Criminal Justice Act 1988 (CJA88): This is amended by the CJA93 to include certain money laundering crimes.

B Prevention of Terrorism (Temporary Provisions) Act 1989 (POTA): This contains a similar provision to that which pertains under the drug trafficking legislation. However, it relates to terrorist funds and is significant in that the legislation applies to terrorist activities committed anywhere in the world, and allows for prosecution in the UK.

B Criminal Justice (International Co-operation) Act 1990 (CJICA): This Act introduced new kinds of money laundering offences but these still only relate to the proceeds of drug trafficking. This Act is also the principle source of mutual assistance powers in the UK given to foreign jurisdictions.

B Criminal Justice (Confiscation) (Northern Ireland) Order 1990 (CJO): This order establishes for Northern Ireland drug money laundering offences equivalent to those in section 49 and 50 of the DTA 1994.

B Northern Ireland (Emergency Provisions) Act 1991 (NIEPA): This measure was needed in order to have specific legislation pertaining to specific terrorist-related acts committed within the province. Has some similar money laundering provisions as those contained in the POTA.

B Criminal Justice Act 1993 (CJA93): This act is the one which creates the modern offence of money laundering. It is significant that this legislation has been shaped to take account of the EU Directive (1991) which itself was based on the 1988 UN Drugs Convention, the Basle Statement of Principles, recommendations of the G7 Financial Action Task Force and the Council of Europe Laundering Convention. It created various offences and exported them to the Acts dealing with Drugs Trafficking and Terrorism. It is also significant in that it creates offences which relate to the laundering of money which is the proceeds of criminal conduct other than drugs trafficking and terrorism. One of the implications of this Act is that you can be prosecuted in the UK for laundering the proceeds of criminal conduct even though the conduct all took place overseas. The biggest revolution however is that this Act creates, for the
first time except under emergency powers, a law that imposes an obligation to report someone else to the police - i.e. the obligation to report a person suspected of money laundering.

Drug Trafficking Act 1994: This is new law replacing DTOA86. This was brought about to update the law regarding drugs. New money laundering provisions are included to close the loopholes identified by Home Affairs Committee on Organized Crime.

Criminal Law (Consolidation) (Scotland) Act 1995: This Act brought Scotland into line with English legislation. Some sections were derived from the CJA93. The Act also implements certain articles taken from the EU Directive (1991) with yet other sections which equate to sections of the DTA94.

The Proceeds of Crime (Scotland) Act 1995: This relates to confiscation and forfeiture of criminally derived proceeds. The primary aim of this legislation being that the offender should not be allowed to retain any benefit from their crime.

Primary legislation is of general public application and is not specifically aimed at financial institutions.

The Proceeds of Crime Act (POCA) 2002: The Proceeds of Crime Act updated, expanded, and reformed the criminal law in the U.K with regard to money laundering.


- provide more detailed obligations regarding customer due diligence, for example, explicit requirements for firms to undertake ongoing monitoring of business relationships and for firms to identify not just the customer but the beneficial owner of the customer;

- require firms to vary customer due diligence and monitoring according to the risk of money laundering or terrorist financing;
require firms to take enhanced customer due diligence measures in higher risk situations, while allowing firms to take reduced identification measures for specific situations with a lower risk of money laundering;

allow firms to rely on certain other firms for undertaking customer identification; and

clarify the arrangements for the supervision of firms, including those that will be supervised for the first time.

Most UK financial firms (banks, building societies, money transmitters, bureaux de change, cheque cashers, savings and investment firms) are covered. In addition the Regulations cover legal professionals (when undertaking some activities) accountants, tax advisers, auditors, insolvency practitioners, estate agents, casinos, high value dealers when dealing in goods worth over 15,000 Euro and trust or company service providers.

U.S

The U.S. has imposed many legislative and regulatory standards to help deter money laundering. The most significant of these are:

The Bank Secrecy Act (Currency and Foreign Transactions Reporting Act of 1970): The Bank Secrecy Act (BSA) was designed to fight drug trafficking, money laundering, and other crimes. Congress enacted the BSA to help prevent banks and other financial service providers from being used as intermediaries for, or being used to hide the transfer or deposit of money derived from, criminal activity.¹

Money Laundering Control Act of 1986: It is a United States Act of Congress that made money laundering a Federal crime and is one of the most powerful anti-money laundering laws in the world.

Anti-Drug Abuse Act of 1988: The Anti-Drug Abuse Act of 1988 reinforced and supplemented anti-money laundering efforts by increasing the levels of penalties and sanctions for money laundering crimes and by requiring strict identification and documentation of cash purchases of certain monetary instruments.²

91
Section 2532 of the Crime Control Act of 1990: Section 2532 of the Crime Control Act of 1990 enhanced the federal banking agencies enforcement position by giving it powers to work with foreign banking authorities on investigations, examinations, or enforcement actions dealing with possible bank or currency transaction-related violations.

Section 206 of The Federal Deposit Insurance Corporation Improvement Act (FDICIA) of 1991: The FDICIA allowed the OCC and other bank supervisory authorities some latitude in disclosing to foreign bank regulatory or supervisory authorities information obtained during its supervisory role. Such disclosure must be appropriate, not prejudice the interests of the U.S., and must be subject to appropriate measures of confidentiality (Office of the Comptroller of the Currency, Washington, DC, 2002).

Annunzio-Wylie Anti-Money Laundering Act of 1992: This act increased penalties for depository institutions found guilty of money laundering. The act added several significant provisions to the BSA, including the reporting of suspicious transactions (Office of the Comptroller of the Currency, Washington, DC, 2002).


USA PATRIOT Act: The USA PATRIOT Act evolved as a response by the U.S. government to combat international terrorism. The act contained strong measures to prevent, detect, and prosecute terrorism and international money
laundering. Signed into law on October 26th, 2001, the act establishes new rules and responsibilities affecting U.S. banking organizations, other financial institutions, and non-financial commercial businesses.

**India**

In India, legislation provides for the confiscation or forfeiture of the proceeds or assets of certain crimes. These include: Criminal Law (Amendment) Ordinance, 1944, Customs Act, 1962, Code of Criminal Procedure, 1973, Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act, 1976, Narcotic drugs & Psychotropic Substance Act, 1985.

In addition, Indian Statutes also provide preventive detention of foreign exchange racketeers under the conservation of foreign exchange and prevention of smuggling activities (COFEPOSA) Act, 1974 and the preventive detention of drug traffickers under the prevention of Illicit traffic in Narcotic drugs and psychotropic substances (PITNDPS), Act 1988.

The Foreign Exchange Management Act (FEMA): The Foreign Exchange Management Act, implemented in 2000, is one of the Government of India’s primary tools for fighting money laundering. The FEMA's objectives include establishing controls over foreign exchange, preventing capital flight, and maintaining external solvency. FEMA also imposes fines on unlicensed foreign exchange dealers.

The Prevention of Money Laundering Act (PMLA): The Prevention of Money Laundering Act (PMLA) was signed into law in January, 2003. This legislation criminalizes money laundering, establishes fines and sentences for money laundering offenses, imposes reporting and record keeping requirements on financial institutions, provides for the seizure and confiscation of criminal proceeds, and provides for the creation of a financial intelligence unit (FIU). Implementing rules and regulations for the PMLA were promulgated in July, 2005.

**Iran**

Iran has approved legislative and regulatory to help deter money laundering. Anti Money Laundering Law 2008: Iranian anti-money laundering law was approved by
the Islamic Parliament on January 22\textsuperscript{nd}, 2008 and the Guardian Council on February 6\textsuperscript{th}, 2008. This was the first law to criminalize money laundering. The law creates a High Council on Anti-Money Laundering chaired by the Minister of Economic Affairs and Finance. Membership in the High Council includes the Ministers of Commerce, Intelligence, Interior, and the Governor of the Central Bank of Iran.

Executive by- Law of the Anti- Money Laundering ACT: The Executive by- Law of The Anti- Money Laundering ACT was approved by the president on Dec. 2\textsuperscript{nd}, 2009. This by-law was communicated by the First Vice President to perform the duties by individuals and legal entities subject to it.
3.2 LEGAL REGIME

This part of research gives an overview of the legal regimes of the U.K, U.S, India and Iran and discuss about criminalization of money laundering, confiscation and seizing of proceeds of crime, authorities such as the financial intelligence unit (FIU), and law enforcement.

3.2.1 Criminalization of Money Laundering

According the FATF Recommendation No. 1., “Countries should criminalize money laundering on the basis of United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention).” The Vienna and Palermo conventions require countries to establish as a criminal offense the following intentional acts: conversion or transfer of proceeds; concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to proceeds; and the acquisition, possession or use of proceeds. This obligation is subject to the fundamental/constitutional principles and basic concepts of the country’s legal system.

U.K

In the UK, the current legislation that criminalizes money laundering is the Proceeds of Crime Act (POCA) 2002. The Proceeds of Crime Act updated, expanded, and reformed the criminal law in the U.K with regard to money laundering. The relevant Part 7 provisions, which came into force on 24 February 2003, set out the three principal money laundering offences: Concealing etc. Criminal property: the act of concealing, disguising, converting or transferring criminal property, or removing criminal property from the UK; Arrangements in respect of criminal property: the act of assisting another person to retain, acquire, use or control criminal property through entering into an arrangement to facilitate this objective; and Acquisition, use or possession of criminal property
Before 24th February, 2003, the Proceeds of Crime Act 2002 money laundering was criminalized in terms of two separate pieces of precursor legislation, namely the Criminal Justice Act 1988 and the Drug Trafficking Act 1994. The scope of the money laundering offences under these two pieces of legislation differed in that the Drug Trafficking Act 1994 applied to money laundering in respect of predicate offences relating to drug trafficking while the Criminal Justice Act applied to money laundering in respect of all other predicate offences.

U.S

The U.S. criminalized money laundering on 27th October, 1986. Sections 1956 and 1957 of Money Laundering Control Act 1986 criminalize four different types of money laundering: basic money laundering; international money laundering; money laundering in the context of an undercover "sting" case; and knowingly spending greater than USD 10,000 in criminal proceeds.

India

In India, the constitutional power for legislating with respect to money laundering rests with the Union Government, as it is linked to the banking and external affairs powers in the Constitution. Beyond the relevant section in the Narcotic Drugs and Psychotropic Substances Act 1988, the Prevention of Money Laundering Act 2002 (PMLA) was the first law to criminalize money laundering. There is no State-based money laundering offences.

PMLA amendments introduced a new category of predicate offenses, cross-border crimes such as fraud and theft, with no threshold amount for prosecution. Offenses under the Unlawful Activities (Prevention) Act (UAPA) relating to terrorism and terrorist financing are included as predicate offenses, as are insider trading and market manipulation. Offenses relating to human trafficking, smuggling of migrants, counterfeiting, piracy, environmental crimes, and over- and under-invoicing under the Customs Act have become punishable under the amended.
Iran

Iran criminalized money laundering on January 22nd, 2008. In Iran, Money Laundering consists of:

a) Acquisition, possession, keeping or using the proceeds from illegal activities with the knowledge that they have been acquired directly or indirectly through a criminal offence.

b) Change, exchange, or transfer of proceeds with the intention of hiding their illegal origin with knowledge that they have been acquired directly or indirectly through a criminal offence, or helping the offender in such a way that the legal effects and consequences of the commitment of that crime would not involve him/her.

c) Hiding or covering up the real nature, origin, source, location, movement, displacement, or possession of proceeds obtained directly or indirectly as a result of an offence (Article 2 Anti Money Laundering Law).

In the laws and regulations of Iran, the term terrorism has had little and limited usage. In its place equivalent terms have been used which are in line with the local custom and literature such as "taking up arms to fight the people" and "corrupt on the face of the earth" which have a conceptual meaning equivalent to terrorism and bring to mind intimidation and fear and threats.

3.2.2 Confiscation and seizing of proceeds of crime

The term confiscation, which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the State. In this case, the person or entity that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets. Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision.
whereby the confiscated or forfeited property is determined to have been derived from or intended for use in a violation of the law.

There was from the late 1980’s onwards a resurgence of interest in confiscation as crime prevention tool, which went hand in hand with the interest in the criminalization of Money Laundering. A number of international instruments, starting with the 1988 Vienna Convention, have strongly suggested the enactment of legal provisions enabling confiscation of proceeds of crime. The 40 Recommendations of the FATF have also stated its importance as a crime prevention tool.

A robust system of provisional measures and confiscation is an important part of an effective anti-money laundering regime. Confiscation and seizure prevents criminal property from being laundered or reinvested either to facilitate other forms of crime or to conceal illicit proceeds.

U.K

U.K law provides for the confiscation of laundered property which represents proceeds from, instrumentalities used in, and instrumentalities intended for use in the commission of ML, FT or other predicate offences, and property of corresponding value. There are three principal pieces of legislation providing scope for confiscation and recovery of laundered money or proceeds of crime:

- Proceeds of Crime Act 2002
- Terrorism Act 2000
- Anti-terrorism, Crime and Security Act 2001

Anti-terrorism, Crime and Security Act 2001 provide for the seizure of cash by the police or HMRC where they have reasonable grounds for suspecting that: the cash is intended for use for the purposes of terrorism, or represents the assets of a proscribed organisation, or represents property obtained through terrorism, or is property that has been earmarked as terrorist property (Financial Action Task Force, 2007).
According to the Third Mutual Evaluation Report of the Financial Action Task Force (2006), the federal laws have parallel civil and criminal Confiscation systems, which provide for the Confiscation of both the instrumentalities and proceeds of crime. Administrative forfeiture can also be applied under certain conditions. Confiscation of property is only possible when provided in a specific statute and when related to a large number of offenses specified in 18 USC 981 and 982, including Money Laundering and Terrorism Financing. All property constituting the subject matter of a money laundering offense being subject to forfeiture, the confiscation is not limited to the net profits realized from a sale or exchange, but includes any property that was involved in the offense. Also, when money laundering activity relates to commingled funds, confiscation applies to the commingled funds as “property involved” in the offense. Property subject to confiscation can be seized, frozen or otherwise preserved prior to trial in order to ensure that it remains available, provided that there is probable cause to believe that the property is subject to confiscation. The property can also be seized with a criminal seizure warrant [s.853 (f)] if it is demonstrated that a restraining order would not be adequate to preserve the property. However, only property “involved in” or “traceable to” the offense can be seized. The PATRIOT Act allows the government to seize funds subject to forfeiture which are located in a foreign bank account, by authorizing the seizure of the foreign bank’s funds that are held in a correspondent U.S. account, regardless of whether or not the money in the correspondent account is directly traceable to the money held in the foreign bank account (section 319).

India

In India, provisions that authorize the confiscation, freezing and seizing of proceeds of crime are spread across a number of legislative instruments, depending on what crime the proceeds are derived from.

The Unlawful Activities (Prevention Act) 1967 (UAPA) enables seizure and forfeiture of proceeds of terrorism. The Narcotic Drugs and Psychotropic Substances Act 1985 (NDPS) allows confiscation of illegal property of persons under arrest or convicted of
an offence punishable by 10 years or more under the Act or an order of detention under other listed drug Acts.

Chapter V of the UAPA allows for confiscation of property that is proceeds of terrorist financing but it only covers instrumentalities used in, or intended for use in, terrorist financing in limited circumstances.

Chapter V-A of the NDPS Act allows for the confiscation of proceeds of drug offences under the Act, but only, at the minimum, where a warrant for the arrest of a person has been issued for an offence punishable with imprisonment for more than 10 years.

Chapter III of the PMLA will provide for confiscation of laundered property, but only when there has been a conviction for a scheduled offence. Where it is suspected that a person is in possession of any proceeds of crime and he has been charged with a scheduled offence, and the proceeds of crime are likely to be laundered or dealt with to avoid confiscation, the property can be attached (restrained) for 90 days.

The PMLA allows for attachment of property once a person has been charged with a predicate offence under section 5. Premises can also be searched and property can be seized where there is reason to believe that a person has committed money laundering or is in possession of proceeds of crime related to money laundering.

**Iran**

According to Article 9 of the AML law, “Those who engage in the crime of money laundering will, in addition to returning the assets and the proceeds derived from the crime comprising the original assets and the profits there of (and if nonexistent, the equivalent or the price), be sentenced to a fine of one fourth of the value of the proceeds of the crime which should be deposited into the public Revenues Account with the Central Bank of the Islamic Republic of Iran.” If the proceeds have been converted into other property, that property will be seized. The order to seize the assets and their derived profits can be issued and exercised if the accused “has not been subject to this order under predicate offenses.
3.2.3 The Financial Intelligence Unit (FIU)

Recent efforts to develop effective strategies for anti-money laundering and combating the financing of terrorism bring together several distinct but related aspects of financial systems and criminal law. Financial intelligence units (FIUs) constitute an important component of these strategies (World Bank, 2004). In their simplest form, 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 foreign FIUs to combat money laundering (Figure. 3.6).

The first few FIUs were established in the early 1990’s in response to the need for a central agency to receive, analyze, and disseminate financial information to combat money laundering. Over the following ten years, the number of FIUs increased to the point where the Egmont Group, the informal international association of FIUs, had 94 members in 2004. In 2003, the Financial Action Task Force adopted a revised set of recommendations on combating money laundering that, for the first time, included explicit recommendations on the establishment and functioning of FIUs. According to Recommendation 26 of FTAF, countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

In recent years, recognizing the importance of an FIU in the anti-money laundering/combating the financing of terrorism framework, the International Monetary Fund and the World Bank, as well as a number of their member countries, have provided technical assistance to countries in the establishment and strengthening of FIUs.
The functions of the UK FIU (receiving, analyzing, and disseminating reports relating to money laundering) were first carried out in 1992 by the Economic Crime Unit (ECU) within the National Criminal Intelligence Service (NCIS). On 1st April, 2006, the Serious Organized and Police Act 2005 (SOCPA) created the Serious Organized Crime Agency (SOCA). On the same day, NCIS ceased to exist and SOCA subsumed its functions and resources. Accordingly, the functions of the UK FIU are now within SOCA, and SOCA is responsible for performance management of this unit.
POCA 2002 and the Terrorism Act (TACT) 2000 require persons within the regulated sector to make disclosures in the form of suspicious activity reports (SARs) to SOCA when they know or suspect, or have reasonable grounds to know or suspect that another is engaged in ML and FT. A specific operational division, the Proceeds of Crime Department, has been set up within SOCA to take this forward; the UK FIU sits within the Proceeds of Crime Department. While the law indicates that SARs come to SOCA in general, internal policies and procedures ensure that they come
directly to UK FIU, and are processed, analyzed and disseminated solely by UK FIU staff.

The UK FIU was a founding member of the Egmont Group and granted full membership status in June, 1995. In accordance with Egmont practice, when SOCA took on FIU responsibilities for the UK, it was required to complete a formal application for Egmont recognition. The SOCA submission was assessed by members of the Egmont Legal Working Group in June 2006, who confirmed SOCA’s UK FIU Egmont status.4

Analyzing the SARs

The SARs Control team generally receives and processes SARs, and uses specific search parameters to sort them into certain categories for analysis by specific FIU teams. The teams use further search parameters, data mining, research of other databases, and analytical tools such as link software during their analysis. The FIU is authorized to disseminate financial information to domestic authorities for investigation or action when there are grounds to suspect Money Laundering or Terrorism Financing. All SARs relating to suspected terrorist financing, whether reported under TACT or POCA, are individually analyzed by the Terrorist Financing Team, and if appropriate, disseminated to the National Terrorist Finance Investigation Unit (Financial Action Task Force, 2007).

Reporting

In order to provide guidance to all reporting parties on the use of these methods, SOCA publishes comprehensive guidance on its own website5. The SOCA website also has a preferred form for electronic submission of suspicious activity reports and guidance on completion and submission, including SARs seeking consent. The UK has five methods of reporting:

- “Money Web” Extranet Site: A secure extranet system for electronic reporting and submission of SARs for businesses who report 250+ a year.
- Secure (Encrypted) Email: A secure email system for the electronic reporting and submission of SARs for major reporters.
**SAR Online:** Secure web based reporting/submission system for users not on Money Web, and who typically submit less than 250+ a year.

**The use of data on CD Roms and/or computer disks:** Some organizations’ IT systems prohibit encrypted email traffic as it contravenes their IT security policy. In cases such as these, these organizations can output their disclosures to a disk or CD Rom in an agreed format.

**Hard copy submission:** Postal or fax submission of typed or handwritten SARs using copies of the SOCA Preferred Form, letter, or firm’s own version of SAR.

**Access to information:**

The UK FIU has direct and indirect access to additional financial, administrative, and law enforcement information. The UK FIU has direct access to a number of domestic law enforcement sources, in particular: two other SOCA intelligence databases, the Police National Computer, JARD (The asset recovery database), and the Egmont Secure Web (ESW). There are no time constraints in relation to the FIU’s utilization of these sources. The FIU also subscribes to a wide range of commercial databases and open sources, for example: World Check, GB Accelerator, TV Licensing, credit reference agencies, Telephone Directory Enquiries, Dunn & Bradstreet companies data, and Factiva (a media website collating open source reporting). The FIU also has indirect access to operational, regulatory, and public record information maintained by other agencies: Interpol; HMRC databases; HM Prison Service; Department for Work and Pensions (distributor of social security payments); Land Registry; Companies House; Charity Commission; Driver Vehicle Licensing Authority; Local Authorities; UK Passport Agency; and the Public Records Office (FATF, 2007).

**U.S**

The U.S. Department of the Treasury established the Financial Crimes Enforcement Network (FinCEN) in 1990 to provide a government-wide multisource financial intelligence and analysis network. The organization's operation was broadened in 1994 to include regulatory responsibilities for administering the Bank Secrecy Act, one of the nation's most potent weapons for preventing corruption of the U.S.
financial system. The Bank Secrecy Act (BSA), enacted in 1970, authorizes the Secretary of the Treasury to require certain records or reports where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism. The authority of the Secretary to administer Title II of the Bank Secrecy Act has been delegated to the Director of the Financial Crimes Enforcement Network. The USA PATRIOT Act of 2001, enacted shortly after the 9/11 attacks in America, broadened the scope of the Bank Secrecy Act to focus on terrorist financing as well as money laundering. The Act also gave the Financial Crimes Enforcement Network additional responsibilities and authorities in both important areas, and established the organization as a bureau within the Treasury Department.

The mission of FinCEN is to fulfill the duties and powers assigned to the Director by the USA PATRIOT Act, support law enforcement efforts, foster interagency and global co-operation against domestic and international financial crimes, and provide U.S. policy makers with strategic analysis of domestic and worldwide trends and patterns. FinCEN support federal, state, local and international law enforcement. FinCEN works toward those ends through information collection, analysis and sharing, as well as technological assistance and innovative, cost-effective implementation of The BSA and other Treasury authorities that have been assigned to it. FinCEN is considered to be law enforcement support agency, although it has no criminal investigative or arrest authority. As the sole administrator of the BSA, FinCEN retains a high-degree of operational independence.
FinCEN is responsible for collecting, housing, analyzing and disseminating financial information that is collected under the BSA and other authorities, and which relates to investigations of illicit finance (including money laundering). The duties and powers of FinCEN expressly include “analyzing and disseminating the available data...to determine emerging trends and methods in money laundering and other financial crimes” (Bank Secrecy Act: 31 USC 310(b) (2) (C)) among other things, and to gain an increased understanding of methodologies, typologies, geographic patterns of activity and systemic vulnerabilities relating to terrorist financing (Financial Action Task Force, 2006).

Access to information

The information that FinCEN collects under the BSA and the ability to link this data with a variety of law enforcement and commercial databases makes FinCEN one of the largest repositories of information available to law enforcement in the country.
FinCEN’s information sources fall into three categories, all of which can be accessed by FinCEN in a timely manner:

(1) Direct access to its financial database;

(2) Direct access to commercial databases; and

(3) Indirect access to law enforcement data.

FinCEN also has the authority to go to reporting parties for additional information directly or through law enforcement.

**Guidance concerning the obligation to report**

According to the Financial Action Task Force in Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism (2006), FinCEN provides various types of guidance and general feedback to domestic Financial Institutions and DNFBPs regarding the detection and reporting of suspicious activity. FinCEN’s guidance materials include the following:

- letter rulings explaining how SAR requirements apply to specific facts and circumstances;
- answers to frequently asked questions about SAR requirements;
- a document entitled “Guidance on Preparing a Complete and Sufficient Suspicious Activity Report Narrative”;
- a document entitled “Suspicious Activity Reporting Guidance for Casinos”; and
- SAR Bulletins on specific issues, like automatic teller machines, phone cards, indicators of the financing of terrorism, and SARs filed by casinos;
- the annual “SAR Activity Review—Trends, Tips & Issues and its companion publication “SARs by the Numbers”.
India

Financial Intelligence Unit – India (FIU-IND) was set by the Government of India on 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. Notification number 5/2005 dated 1st July, 2005 confers powers on the Director of FIU-IND. Trehan (2009) believes that the roles of Intelligence are critical for success in the fight against ML.

Figure 3.9 FIU-IND structures

According to the Annual report of Financial Intelligence Unit – India (2008), FIU-IND is a multi disciplinary body with a sanctioned strength of 43 personnel. These are being inducted from different organizations namely Central Board of Direct Taxes
The FIU-IND is not intended to operate as an investigate unit. Its primary role will be to receive process and analyse the cash and suspicious transactions reports and then forward these reports to the appropriate enforcement agency for action as required. Transactions that appear to be related to money laundering offences under the PMLA will be passed to Directorate of Enforcement for investigation.

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

- **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 FIU.

- **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.
Iran

According to Anti-money laundering law of Iran, the financial intelligence unit was set up in the Ministry of Economic Affairs and Finance to fulfill the functions set out below:

- To gather, collect and obtain information on the suspicious transactions;
- To evaluate, examine and analyze the information in the reports and about suspicious transactions;
- To enter and classify the information in the mechanized system;
- To report the particulars of the persons involved in money laundering activities and/or in terrorist financing to the designated persons to exercise more caution and/or terminate cooperation if requested by the appropriate authorities;
- To provide the analyzed information by judicial authorities, officers and establishments in charges of fight against terrorism in the country if requested by the appropriate authorities;
- To prepare the required statistics from the measures carried out in the anti-money laundering process;
- To procure the required software and information systems;
- To provide security for the collected information;
- To exchange information with international organizations and institutions subject to the rules;
- To gather and obtain international experiences;
- To send reports with a high probability of accuracy or when their probability will be of great importance to the judicial authorities;
- To follow up the transmitted reports with the judicial authorities;
- To prepare the draft annual plan of the financial intelligence unit for the Council’s approval;

- To send responses to the inquiries made by the designated persons as soon as reasonably practicable;

- To comment on the professional qualifications of the administrators of anti-money laundering units proposed by the directors of the designated competent authorities.

According to Article 39 of Executive by-Law, Appointment and dismissal of the secretary shall take place upon the recommendation of the Minister of Economic Affairs and Finance, Council’s approval and upon the ordinance given by the Minister of Economic Affairs and Finance. The financial intelligence unit shall perform its functions under the direction of the secretary. All posts at the Supreme Council Secretariat (SCS), financial intelligence unit and affiliated units shall be considered as sensitive jobs and shall be consistent with the appropriate rules.

All designated persons shall have to provide the information requested by the financial intelligence unit regarding the anti-money laundering activities in a manner established by such unit to perform the assigned duties (Article 47 of Executive by-Law of The Anti-Money Laundering ACT).

### 3.2.4 Law enforcement

**U.K.**

The Financial Action Task Force (2007) in the Third Mutual Evaluation on Anti-Money laundering and combating the Financing of Terrorism Reported, all law enforcement agencies, including: all UK police forces, SOCA, HMRC, and SCDEA have responsibility for ensuring that money laundering offences are investigated, and have permanent specialist financial crime teams available for such investigations. All law enforcement agencies have a dedicated financial intelligence unit for assessing SARs disseminated by the UK FIU and analysis of other financial intelligence. In some cases, regional FIUs are part of the financial investigation unit / economic crime
unit that carries out financial investigations for that force or agency. An investigator can arrest a person at any time when he has reasonable grounds to suspect the person has committed an offence. Law enforcement and other competent authorities are:

- There are 43 regional police forces in England and Wales that they have specialist financial crime investigation units.
- The City Of London Police that has a large Financial Investigation Unit, as part of the Economic Crime Department.
- The NTFIU that is a multi-agency body consisting of financial investigators dedicated to combating terrorist financing. It is part of a Special Branch (SO-15) of the Security Service.
- SOCA that has an enforcement capability specifically dedicated to tackling money laundering and asset recovery. These financial investigators however remain part of the Proceeds of Crime Department (PoC) command structure to ensure operational independence and freedom from undue influence within the Enforcement Teams.
- HMRC that has approximately 274 Financial Investigators. There is a specialist Financial Investigation Division which comprises three distinct commands.
- Crown Prosecution Service (CPS) that is responsible for prosecuting criminal cases investigated by the police in England and Wales, including advising the police on cases for possible prosecution, and review, prepare and present cases in court.
- Scottish Crown Office and Procurator Fiscal Services (COPFS) that is prosecute all crime in Scotland.
- Revenue and Customs Prosecution Office (RCPO) that is an independent government department responsible for prosecuting all HMRC criminal cases in England and Wales.
Public Prosecution Service of Northern Ireland (PPSNI) that is prosecutes criminal cases investigated by police, HMRC, and SOCA in Northern Ireland.

The Scottish Crime and Drug Enforcement Agency (SCDEA) Money Laundering Unit (“SMLU”) that is led by a Detective Inspector backed up a 12-strong team, including one dedicated financial analyst.

The Assets Recovery Agency (ARA) that has offices in London and Belfast.

Under the Proceeds of Crime Act 2002, the Director of the Assets Recovery Agency (ARA) has a statutory duty to train, accredit and monitor the accreditation of financial investigators throughout England, Wales, and Northern Ireland. ARA accreditation is the only recognized accreditation for financial investigators in the UK.

U.S

The Financial Action Task Force in Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism (2006) reported that, Law enforcement in the U.S is one of three major components of the criminal justice system, along with courts and corrections. The U.S. Constitution places responsibility for the investigation and prosecution of federal crimes in the executive branch. Investigatory jurisdiction for the crime of money laundering rests by statute with the Treasury, the DOJ, DHS, and the Postal Service.

Department of Justice (DOJ): The DOJ is the central authority for the investigation and prosecution of federal laws in the U.S., including the federal money laundering and terrorist financing offenses.

Federal Bureau of Investigation (FBI): Primary investigative responsibility for the investigation of terrorism and terrorist financing rests with the FBI-led multi agency JTTF. The FBI has specialized units located at their Headquarters in Washington DC for investigating terrorist financing. Additionally, the FBI promotes the investigation and prosecution of money laundering across all investigative programs in which it participates.
Immigration and Customs Enforcement (ICE): ICE is the largest investigative agency in the Department of Homeland Security. Formed in 2003 as part of the federal government's response to the 9/11 attacks, ICE's mission is to protect the security of the American people and homeland by vigilantly enforcing the nation's immigration and customs laws. ICE is responsible for deterring, interdicting, and investigating threats arising from the movement of people and goods into and out of the U.S. This includes investigating bulk cash smuggling, drug smuggling, alien trafficking and commercial fraud. ICE targets the financial component of all investigations within its areas of jurisdiction. ICE has made it a priority to target the financial component to all investigations of criminal activity within its areas of jurisdiction, including narcotics smuggling, alien trafficking and commercial fraud.

Drug Enforcement Administration Office of Financial Operations (FO): The Drug Enforcement Administration (DAE) was created by President Richard Nixon through an Executive Order in July 1973 in order to establish a single unified command to combat "an all-out global war on the drug menace." The FO is the primary office responsible for the monitoring of money laundering/financial investigations within DEA. It provides the field with guidance on how to best utilize approved money laundering operations and plans initiatives to include the evaluation, auditing, and monitoring of all financial investigations and approved money laundering operations.9

Customs and Border Protection (CBP): The CBP is one of the Department of Homeland Security’s largest and most complex components, with a priority mission of keeping terrorists and their weapons out of the U.S. It also has a responsibility for securing and facilitating trade and travel while enforcing hundreds of U.S. regulations, including immigration and drug laws.

Internal Revenue Service Lead Developmental Centers (LDC): The IRS is the US agency that collects taxes and enforces the internal revenue laws. It is an agency within the U.S. Department of the Treasury and is responsible for interpretation and application of Federal tax law. The IRS-CI has implemented specialized centers—the LDC—to develop cases for investigations. The LDC
has sufficient procedures in place to control and monitor the promoter investigations from start to finish.\textsuperscript{10}

Additionally, many of the law enforcement agencies have units that specialize in investigating the proceeds of crime and are staffed with trained financial investigators. For example, the DEA’s FO focuses on the financial component of drug investigations. Numerous interagency working groups and task forces also specialize in money laundering and terrorist financing investigations, such as the HIFCAs\textsuperscript{11} (for ML) and the JTTFs\textsuperscript{12} (for FT). Other interagency working groups focus on intelligence sharing. Additionally, special units, such as the AFMLS\textsuperscript{13}, have been established to focus on the seizure, freezing and confiscation of the proceeds of crime.

**India**

Law enforcement in India is conducted by numerous law enforcement agencies. At the union (federal) level, the agencies are part of the Union Ministry of Home Affairs, and support the states in their duties.

According to section 54, certain officers are empowered and required to assist the authorities in the enforcement of the PMLA, including:

- officers of the Customs and Central Excise Departments
- officers appointed under sub-section (1) of section 5 of the Narcotic Drugs and Psychotropic Substances Act, 1985 (61 of 1985);
- income-tax authorities under sub-section (1) of section 117 of the Income-tax Act, 1961 (43 of 1961);
- officers of the stock exchange recognised under section 4 of the Securities Contracts (Regulation) Act, 1956 (42 of 1956);
- officers of the Reserve Bank of India constituted under sub-section (1) of section 3 of the Reserve Bank of India Act, 1934 (2 of 1934);
- officers of Police;
- officers of enforcement appointed under sub-section (1) of section 36 of the Foreign Exchange Management Act, 1973 (40 of 1999);
of the Securities and Exchange Board of India established under section 3 of the Securities and Exchange Board of India Act, 1992 (15 of 1992);

- officers of any other body corporate constituted or established under a Central Act or a State Act;

- such other officers of the Central Government, State Government, local authorities or banking companies as the Central Government may, by notification, specify, in this behalf."

The Directorate of Enforcement within the Ministry of Finance will be the designated law enforcement unit to investigate and prosecute money laundering offences and to provisionally attach the proceeds of crime and seize incriminating materials. Investigation officers are empowered with the power of survey, search and seizure, search of persons and arrest if there is reason to believe that a money laundering offence has been committed.

The Directorate of Enforcement advises that it intends to reorganize its structure so as to assume the responsibility for investigation of money laundering offence and attachment of proceeds of crime in addition to its responsibilities administering the Foreign Exchange Management Act (FEMA). The Directorate of Enforcement is also responsible for investigations into terrorist financing where there is contravention of the FEMA.

In addition to the State police, the Narcotics Control Bureau (NCB) and the Central Bureau of Investigation (CBI) are the Union investigation units that deal with the predicate offences under the PMLA. The CBI is Indian’s premier investigative agency, responsible for a wide variety of criminal and national security matters. It was established on 1st April, 1963 and evolved from the Special Police Establishment founded in 1941.
Iran

Iran through the Ministry of Economic Affairs and Finance (MEAF) and Central Bank of the Islamic Republic of Iran (CBI) is committed to ensuring that businesses operating in Iran are legitimate and conduct their business in accordance with the set rules and regulations that protect the companies, their shareholders and their clients from the activities of unscrupulous operators and criminals.

An office has been established in the MEAF through which all businesses and individuals can learn about ML issues, avail themselves of assistance, and file STRs.

The CBI is a state-owned institution established in 1960. It operates in accordance with the Monetary and Banking Act of Iran (MBAI) and its amendments. The CBI supervises the Iranian banking sector. CBI has introduced anti-money laundering measures (‘Anti-Money Laundering Act’ of 2003 and the ‘Regulations Concerning Prevention of Money Laundering through Financial Institutions’).

Law enforcement in Iran served under the Ministry of Interior and Justice. According to the law, Police Force, as the constable of the judiciary, is in charge of the following responsibilities:

- Investigation and detection
- Preventing crime
- Crime detection
- Fight against drugs
- Fight against illicit
- Fight against corruption and unlawful activities
- Arresting convicts and culprit
- Identifying and scientific crime detection.
- Protecting and controlling the borders of Islamic Republic Of Iran, enforcing treaties and
Protocols and supporting the government and residence of the borders rights.

Upholding order and security and maintaining public welfare

According to AML law (Article 11) all affairs which shall, in the execution of law, require a judicial action or authorization shall be performed in accordance with the rules in force. The Judiciary shall have to provide cooperation as per the regulations. Certain branches of the public courts in Tehran and, in provincial capitals, shall be specifically mandated to investigate the money laundering offence and related crimes.
3.3 PREVENTIVE REGIME

3.3.1 Financial Institutions

FATF Recommendations 5-16 and 21-22 state that financial institutions or designated non-financial businesses and professions should take certain actions. These references require countries to take measures that will oblige financial institutions or designated non-financial businesses and professions to comply with each Recommendation. The basic obligations under Recommendations 5, 10 and 13 should be set out in law or regulation, while more detailed elements in those Recommendations, as well as obligations under other Recommendations, could be required either by law or regulation or by other enforceable means issued by a competent authority.

“Financial institutions” means any person or entity 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. (This also captures private banking.)
2. Lending. (This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfaiting).)
3. Financial leasing. (This does not extend to financial leasing arrangements in relation to consumer products.)
4. The transfer of money or value. (This applies to financial activity in both the formal or informal sector e.g. alternative remittance activity. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds).
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, CDs, 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.
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. (This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).)

### 3.3.1.1 Risk of money laundering

**U.K**

The Money Laundering Regulations (MLRs), Proceeds of Crime Act 2002 and the Terrorism Act apply to all FIs carrying out financial activities. In addition, the requirements in the MLRs 2007 also apply to all activities. In UK the risk-based approach applies to two main areas:

- JMLSG Guidance and the risk-based approach by firms.
- FSA Supervision.

**U.S**

The U.S financial sector is extremely large and diverse. The definition of "financial institution" within the BSA encompasses not only core financial service providers, but also a range of non-financial businesses. The application of the BSA requirements to all financial activities is subject, in all cases, to the promulgation of implementing regulations. A number of these institutions have been subjected to AML Program
requirements since enactment of the BSA, and more have been incorporated since the enactement of the USA PATRIOT Act.

The USA PATRIOT Act requires a financial institution to implement an anti-money laundering program that has, at a minimum, the following four requirements:

- Policies, procedures and controls designed to detect and prevent money laundering;
- A compliance officer whose role is to oversee the program;
- Training for employees on how to detect and prevent money laundering; and
- Periodic audits of the anti-money laundering program.

According to Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism (2006), the Extensive reference is made to various types of guidance issued as following by the regulatory agencies with respect to the financial sector's AML/CFT obligations and the regulators' approach to compliance. These are including:

- FFIEC BSA AML Examination Manual
- Interpretive guidance published in the Federal Register
- Guidance issued by SROs to Securities Sector Participants
- Interagency guidance
- Advisories

India

Financial Institutions under PMLA includes:

A. FIs as defined in Section 45-I of the RBI Act. RBI regulates and supervises 8 All-India FIs namely Export-Import Bank of India (EXIM Bank), National Bank for Agriculture and Rural Development (NABARD), National Housing Bank (NHB), Small Industries Development Bank of India (SIDBI), Industrial Finance Corporation of India (IFCI Ltd.), Infrastructure Development Finance Company Limited (IDFC
Ltd.), Industrial Investment Bank of India Limited (IIBI Ltd.) and Tourism Finance Corporation of India Ltd (TFCI Ltd).

B. Insurance companies

- Hire Purchase companies,
- Chit fund companies as defined in the Chit Funds Act
- Co-operative banks
- Housing finance institutions as defined in the National Housing Bank Act such as HDFC
- Non-banking financial companies as defined in section 45-I of the RBI Act such as private finance
- Companies - motor and general, hire purchase companies, leasing companies, investment companies etc.

The general principle appears to be that the same minimum standard will be applied to all relevant financial institutions, as covered by the Reserve Bank of India (RBI), but the appropriate laws and regulations have yet to be rolled out in anything near a comprehensive fashion. An emphasis on risk-based procedures is a feature of the guidelines published by the RBI, but this is only in relation to enhanced due diligence requirements for high risk customers, rather than any discretionary derogation from the minimum identification requirements for "normal" risk customers (FATF, 2005).

Iran

In Iran FIs means banks, non-bank credit institutions, credit cooperatives, interest-free loan funds, leasing companies, investee companies, foreign exchange office and other individual and entities that act intermediaries to exchange funds.

The majority of institutions such as banks (including Iranian banks and branches and subsidiaries of foreign banks based in the Islamic Republic of Iran), non-bank credit institutions, credit cooperatives, interest-free loan funds (Qardh al hasanah- a benevolent loan free from Riba- usury), leasing companies, investee companies, foreign exchange office and other individual and entities that act intermediaries to
exchange funds are subject to the full range of AML requirements, including requirements to file SARs, to maintain records of bank and cashier’s check purchases and funds transfers, and all other required transactions, and to implement AML compliance and customer identification programs.

### 3.3.1.2 Customer due diligence

According to Recommendation 5 of FATF, FIs should not keep anonymous accounts or accounts in obviously fictitious names. FIs should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:

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

According to Basel Committee on Banking Supervision Customer identification is an essential element of KYC standards. Banks should establish a systematic procedure for identifying new customers and should not establish a banking relationship until the identity of a new customer is satisfactorily verified. Also, according to Wolfsberg AML Principles, bank should take reasonable measures to establish the identity of its clients and beneficial owners and should only accept clients when this process has been completed.

Comprehensive customer due diligence programs (CDDP) is financial institutions’ most effective weapons against being used unwittingly to launder money or to support terrorist financing. Knowing customers, including depositors and other users of bank services, requiring appropriate identification, and being alert to unusual or suspicious transactions can help deter and detect money laundering and terrorist financing.
schemes. Effective due diligence systems are also fundamental to help ensure compliance with suspicious activity reporting regulations.

**U.K**

The customer identification obligation is set out in the Money Laundering Regulations, which require that new customers are identified satisfactorily, without specifying how FIs should do this; in general they simply require that new customers are identified satisfactorily. Money Laundering Regulations requires that the financial institution must maintain identification procedures which:

(a) require that as soon as is reasonably practicable after contact is first made between the financial institution and the customer (i) the customer must produce satisfactory evidence of his identity; or (ii) such measures specified in the procedures must be taken in order to produce satisfactory evidence of the customer's identity… Moreover, the Joint Money Laundering Steering Group (JMLSG) Guidance\textsuperscript{15} refers to the need to adopt a risk-based approach to customer due diligence.

In U.K, the financial services sector has to be seen in three parts, which are each dealt with differently based on different approaches by the legislator and regulator. Some are overlapping:

The Financial Services Authority (FSA)\textsuperscript{16} regulated sector and some additional practitioners (leasing): Here, the industry itself considered how firms can best comply with that requirement; this is set out in the Treasury approved JMLSG Guidance; The HMRC\textsuperscript{17} supervised sector which is covered by the HMRC Guidance; and the rest, who have no further obligation and no supervision or oversight for AML.

**Anonymous accounts**

According to Money Laundering Regulation 4(3) (a) anonymous, numbered and fictitious named accounts are not allowed to exist in the UK, by requiring that the customer “produce satisfactory evidence of his identity; or that such measure specified in the procedures must be taken in order to produce satisfactory evidence of the customer’s identity.”
When CDD is required

Money Laundering Regulation requires identification when (1) establishing a business relationship; (2) for occasional transactions above the threshold of EUR 15,000; and (3) in case of suspicion of money laundering.

Legal persons, legal arrangements and beneficial ownership

According to MLRs Regulation 4(3) (d), financial institution must maintain identification procedures which…require that where the customer acts or appears to act for another person, reasonable measures must be taken for the purpose of establishing the identity of that person. This is the general requirement to identify the person acting on behalf of another person in all cases, covering both the case of acting for a legal person and acting on behalf of any other customer as well.

JMLSG Guidance provided complete guidance on identification requirements for non-personal customers and legal persons, covering a wide range of entities in detail, with a practical detailed list of ways to achieve identification.

JMLSG guidance generally covers understanding the ownership and control structure of a legal person. Pursuant to JMLSG Guidance consistent with the risk assessment, the firm should fully understand the company’s legal structure and ownership, and should obtain sufficient additional information on the nature of the company’s business, and the reasons for seeking the product or service.

Purpose for the account

There is no explicit obligation to obtain information on the purpose and nature of the business relationship in the UK in all cases (FATF, 2007). The UK authorities explained that in order to comply with the reporting obligations under section 330 and 331 the Proceeds of Crime Act 2002 (POCA) and section 21A of the Terrorism Act 2000 (TACT) and for FSA firms the regulatory requirements under SYSC 3.2.6R and 3.2.6A R, FIs will need to have a clear understanding of their customer’s business to be able to fulfill their duty to report suspicious activity.
Ongoing due diligence

Financial Action Task Force (2007) reported that, in the U.K is no specific requirement in law or regulation to conduct ongoing monitoring or ongoing due diligence. Nor is there a general requirement that ongoing due diligence should include scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution’s knowledge of the customer, their business and risk profile, and where necessary, the source of funds. But according to JMLSG guidance FIs must establish appropriate procedures of internal control for the purposes of forestalling and preventing money laundering/terrorist financing.

Customer risk

Financial Action Task Force (2007) reported that, the MLRs and other legislation do not explicitly address the issue of enhanced due diligence, and there is no general requirement to take additional steps. The FSA Handbook along with the JMLSG Guidance addresses the need for FIs to undertake a risk assessment for its general money laundering and terrorist financing risk and higher risk categories of customer, business relationship or transaction.

Reduced CDD

MLRs Regulation 5 includes a number of exemptions from the identification requirements for low risk situations. These are total exemptions; they are not applicable only in cases of low risk. They cover FIs in the UK, the EEA, and other “comparable” jurisdictions; small life insurance policies where total payments in a year to not exceed EUR 1,000; and pension schemes in certain circumstances. For example, Under the MLR Regulation, verification of the customer identification is not required when the proceeds of a one-off transaction are re-invested for the benefit of the customer of which a record is kept, and which can only result in another reinvestment made on the customer’s behalf or in a payment made directly to the customer (MLR Regulation 5(5)).
Timing of verification

According to the Third Mutual Evaluation Report, Anti – Money laundering and combating the Financing of Terrorism (2007), there is no obligation in law or regulation to verify beneficial ownership, and also there is no obligation to verify the beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. The JMLSG Guidance provides guidance on the commencement of a business relationship before verification of customer ID has taken place, both at a general level, and underpinned by specific sectoral guidance.

Existing customers

There is no enforceable obligation to apply CDD to existing customers. But the JMLSG Guidance: “The FSA reminded firms that, when carrying out risk assessment and mitigation, the FSA would expect them – as part of their overall approach to AML/CFT – to have considered the risk posed by existing customers who have not been identified.”
Box 3. Case study- smuggling

The Case

Three partners opened a business account with a branch of US bank in the UK. The partners were all American citizens; one was a resident of London. The bank followed rigorous know your customer routines and, in line with its policy, also prepared a customer profile/template showing the pattern of transactions predicated from the information provided by the customer.

The partners explained that they were property developers, planning enhanced business in the UK market, hence the need for a local account. Therefore, the customer profile/template predicate funds flowing to and from the US and disbursements within UK. In reality, more than USD 1 million was transferred into the account within a short period of time, all with instructions for immediate transfer to various accounts in Europe. There were little, if any, local UK disbursements.

A disclosure report was made, as this pattern was alien to the customer profile.

The result

The police were interested and quickly made contact with the bank. At their request, the bank called in the customers for clarifications. The police maintained vigilance and eventually arrested the customers. Their real business was not in real estate but in smuggling (Sunder, 2010).

U.S

FIs subject to AML Program rules are required to establish and implement “policies, procedures, and internal controls reasonably designed to achieve compliance with the BSA and the implementing regulations thereunder.” Regulators generally interpret this to require customer identification and verification, monitoring of transactions, and reporting of suspicious activity to appropriate authorities, all as required or appropriate. Section 326 of the USA PATRIOT Act mandated the promulgation of regulations establishing minimum standards for FIs regarding the identification of customers opening new accounts at financial institutions. The implementing regulations require those FIs for which account relationships actually exist to implement reasonable Customer Identification Program (CIP) procedures for:
(1) Verifying the identity of any person seeking to open an account, to the extent reasonable and practicable;

(2) Maintaining records of the information used to verify the person’s identity, including name, address, and other identifying information; and

(3) Determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency.

According to Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism (2006), FinCEN has issued CIP final rules for financial institutions. These rules impose specific requirements in terms of the information that must be gathered at the account-opening stage. The CIP is only one part of a bank’s BSA/AML compliance program. Adequate implementation of a CIP, standing alone, will not be sufficient to meet a bank’s other obligations under the BSA, regulations promulgated by its primary Federal regulator, such as Suspicious Activity Reporting requirements, or regulations promulgated by the Office of Foreign Assets Control.

Anonymous accounts

The BSA requires FIs to identify and verify the identity of customers that open an account. In addition, FIs must identify and verify the identity of customers undertaking certain transactions whether or not an account at the financial institution is involved. This transaction based identification and verification arises when customers engage in large currency transactions, the purchase of certain financial instruments, or certain wire transfers.

When CDD is required

Financial Action Task Force (2006) reported that, the statutory requirement on account-opening procedures has been implemented through regulations. FIs must collect the following identifying information about a customer at the time the customer seeks to open the account: (1) name; (2) for individuals, date of birth; (3) for individuals, a residential or business street address, or, if there is no street address
available, an Army Post Office or Fleet Post Office box number or the street address of next of kin or of another contact individual; or, for persons other than individuals, the principal place of business, local office or other physical location; and (4) for U.S. persons, a U.S. taxpayer identification number; or, for non-U.S. persons, one or more of the following: a U.S. taxpayer identification number, passport number and country of issuance; alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

FIs must also keep records and identifying information pertaining to the sale of bank checks, drafts, cashier’s checks, money orders, and traveler’s checks in excess of USD 3,000 in currency. Verification, in the case of an existing account holder, may be either through a signature card or other file or record at the financial institution, provided the account holder’s name and address were previously verified, or by examination of a document that is normally acceptable within the banking community as a means of identification when cashing checks for non-depositors.

In principle under the FFIEC Manual (2009), if the institution has doubts about the veracity or adequacy of previously obtained customer identification data, then it cannot have a reasonable belief as to the true identity of its customer under the regulation, and must take additional steps to verify the customer’s identity or terminate the account relationship.

**Legal persons, legal arrangements and beneficial ownership**

The Financial Action Task Force in Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism (2006) stated the CIP rules do not require a financial institution to look through a customer that is an entity to its beneficial owners. However, the preamble to the final rule implementing section 326 of the USA PATRIOT Act provides that, based on a bank’s risk assessment of a new account opened by a customer that is not an individual, a bank may need to take additional steps to verify the identity of the customer by seeking information about individuals with ownership or control over the account in order to identify the customer or may need to look through the account in connection with the customer
due diligence procedures required under other provisions of its BSA compliance program.

In related to beneficial owner, the only statutory requirements to identify the beneficial owner before or during the course of establishing a business relationship appear in sections 311 and 312 of the USA PATRIOT Act.

**Purpose for the account**

According to the FFIEC Manual (2009), Management should have a thorough understanding of the money laundering or terrorist financing risks of the bank's customer base. Under this approach, the bank will obtain information at account opening sufficient to develop an understanding of normal and expected activity for the customer's occupation or business operations.

**Ongoing due diligence**

According to FATF (2006), there is no explicit legal requirement to undertake ongoing due diligence in all cases. However, the U.S. authorities interpret the SAR reporting obligations as necessarily requiring institutions to have policies and procedures in place to undertake ongoing due diligence generally. This is based on the fact that the SAR regulations require FIs to report any transaction that “is not the sort in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts . . .” Consequently, the authorities argue this presupposes the existence of ongoing customer due diligence in order for the institution to be able to know what sort of transactions the customer normally undertakes. The FATF standard on ongoing monitoring of accounts requires the obligation to be framed explicitly in law or regulation.

**Reduced CDD**

In terms of reduced CDD options, the CIP rules explicitly do not apply with respect to certain easily identifiable customers, specifically U.S. or State government entities, FIs regulated by a federal functional regulator, banks regulated by a state regulator, and entities whose stock is listed on the NYSE, the American Stock Exchange and the
NASDAQ, provided that, if the entity is a financial institution, the exemption applies only to its U.S. domestic operation (dealings with its foreign offices being subject to normal CIP procedures). In all other cases, institutions are required to apply the CIP rules on a risk-sensitive basis, subject to the minimum requirements laid down in the regulations.

Customer risk

The anti-money laundering program requirements that apply to U.S. FIs are risk-based, requiring institutions to have CDD procedures commensurate with the risk in the business identified by management. To complement this approach, the U.S. has also enacted legislative measures against certain potential higher risk scenarios, requiring enhanced CDD in such cases, thereby strengthening the effectiveness of the AML requirements.

Timing of verification

There is no statutory obligation to complete the verification process before or during the establishment of the relationship. Instead, FIs are required to verify the identity of their customers "within a reasonable time after the account is opened (31 CFR 103.121 for banks)."

Existing customers

According to the Financial Action Task Force (2006), there is no obligation to apply the formal CIP procedures to Existing customers. According to guidance provided by the Federal Banking Agencies on 28th April, 2005 this principle applies also when an existing client opens a new account with the same institution. In the same guidance, the agencies indicated their interpretation as to how an institution could demonstrate that it had a reasonable belief that it knows the true identity of an existing customer.

Politically exposed persons (PEP)

FIs are required, as part of their AML Program to implement procedures for identifying potentially high-risk customers and products. The FFEIC Manual (2010) advises that banks should specifically identify PEP accounts and assess the degree of risks involved.
India

Section 12(1) (c) of the PMLA imposes an obligation on all covered institutions to verify and maintain the records of the identity of all its clients, in such manner as may be prescribed. The corresponding rule (Verification and Maintenance of the Records of Identity of the Clients of Banking Companies, FIs and Intermediaries), to be issued under section 73 of the Act, requires every such institution, at the time of opening an account or executing any transaction, to verify the identity, address, nature of business and financial status of the client.

The RBI has made Know Your Customer (KYC)/CDD guidelines applicable to Scheduled Commercial Banks (with effect from November 2004), Co-Operative Sector and Regional Rural Banks (RRBs) (with effect from February 2005), Non-banking Finance Companies (with effect from October, 2005) and to authorized full-fledged money changers (with effect from December, 2005). Further, under Section 35 of the Banking Regulation (BR) Act, the RBI looks into issues related to KYC and AML while carrying out Annual Financial Inspection of the banks, and comments on them in their reports. The Securities and Exchange Board of India (SEBI) also requires all registered intermediaries to follow detailed CDD measures and to develop customer acceptance policies and procedures that aim to identify the types of customers that pose a higher-than-average risk of money laundering or terrorist financing. Under the guidelines on AML Program for Insurers, issued on March 31, 2006 by Insurance Regulatory and Development Authority (IRDA), insurance companies are required to have in place an AML program that addresses the key requirements of KYC norms.

In October 2009, the Reserve Bank of India strengthened its “Know Your Customer Norms/Anti Money Laundering Standards/Combating of Financing of Terrorism” guidelines by issuing notifications to all banks and FIs on appropriate procedures regarding customer identification and verification. Entities covered by KYC regulations include banks, securities firms and broker dealers, insurance companies, authorized money changers (money remitters, bureaus de change, money changers) and payment systems operators. In November , 2009, the RBI tightened the KYC norms for authorized money transfer service agents, requiring enhanced due diligence
for new customers based on a customer’s risk profile and increased monitoring of receipts considered especially risky based on indicators such as country of origin, sources of funds, and type of transaction. The RBI also has directed banks to take additional precautions on customers’ business transactions with entities or banks from Iran, Pakistan, Uzbekistan, Turkmenistan, and Sao Tome.

According to Know Your Customer (KYC) Norms/Anti-Money Laundering Measures/Combating of Financing of Terrorism /Obligations of banks under PMLA, 2002 guidelines Banks should frame their KYC policies incorporating the following four key elements:

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

Every bank should develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. For the purpose of KYC policy, a ‘Customer’ is defined as:

- a person or entity that maintains an account and/or has a business relationship with the bank;
- one on whose behalf the account is maintained (i.e. the beneficial owner);
- beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
- 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.
Anonymous accounts

According to KYC/AML/CFT guidelines banks are not allowed to open the account of anonymous or fictitious name(s).

When CDD is required

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

Legal persons, legal arrangements and beneficial ownership

According to KYC/AML/CFT guidelines (2009), 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 authorized 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 bank also 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.

Purpose for the account

Banks should keep in mind that the information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Banks should, therefore, ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer should be sought separately with his/her consent and after opening the account (KYC/AML/CFT guidelines, 2009).
**Ongoing due diligence**

The Board of Directors of the 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 and apply various anti money laundering measures keeping in view the risks involved in a transaction, account or banking/business relationship (KYC/AML/CFT guidelines, 2009).

**Customer risk**

Banks should introduce a system of periodical updating of customer identification data (including photograph/s) after the account is opened. The periodicity of such updating 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. 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 categorised as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to the 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 categorised 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. 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; (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 customer (KYC/AML/CFT guidelines, 2009).

**Timing of verification**

Every banking company, financial institution and intermediary shall at the time of commencement of an account-based relationship, identify its clients, verify their identity and obtain information on the purpose and intended nature of the business relationship. In all other cases, identity should be verified while carrying out: (i) transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or (ii) any international money transfer operations.

**Politically exposed persons (PEP)**

Politically Exposed Persons” (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories. 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 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.
Iran

According to Article 7 (a) of ML law, Individuals and organizations subject to this law are obligated to verification of the identity of the client, and where relevant verification of the identity and relationship of the client's representative or proxy, as well as verification of the identity of the principal, in case there are evidences of offence.

AML Executive By-law Article 2 stated that, the credit institutions, insurance companies and the stock exchange company shall have to take action for the initial identification of the client (perform customer due diligence) and enter the relevant information in their database system at the time of providing all kinds of services and dealings in monetary and financial operations even less than the applicable designated threshold such as any type of receipt and payment, money order, drawing and payment of checks, granting loans/ facilities, issuance of various plastic cards, issue of letters of guarantee (LGs), buying and selling foreign currencies, certificates of deposit (CDs) and participation certificates, accepting guarantee and guarantor's obligations in any manner including the signing of promissory notes, bills of exchange and letters of credit (LCs), securities purchase and sale. 19

In accordance with this By-Law, all persons subject to the By-Law are bound to execute the procedures for the initial identification of customers in any transaction, operation and services provided for them over the entitled limit or if they are suspicious of money laundering. According to this regulation, the initial identification will be carried out based on the customer national code and postal code of residence and its compliance with the original ID card (locally called: "Melli Card "). For foreign nationals, this will be done through a valid passport enjoying residence license (permit) or identification card or valid foreign logistics paper.

When CDD is required

According to AML Executive By-law, all designated persons shall have to make the initial identification of their customers at the time of performing any operations as well as providing services above the applicable designated threshold and/ or when suspicion is aroused in respect of money laundering activities.
Initial identification for natural persons

The initial identification of natural person shall take place on the basis of the national code and checking it with the original card as a common practice as well as the zip (postal) code of the place of residence;

Where the designated persons are connected on line to the State Organization of Civil Status Registry for checking information via this channel, the receipt of photo- affixed birth of certificates or driving licenses or valid passports shall not meet any impediment.

With respect to the aliens, the valid passport of the respective country having the entry visa and residence permit or identity card and/ or a valid work permit for aliens shall be regarded as identification records.

The fulfillment of all duties described in the executive by- law of the law requiring the allocation of national code and zip (postal) code of the Iranian citizens shall accordingly be mandatory.

Full identification of natural persons

Pursuant to AML Executive By-law, in addition to the initial identification, the designated persons shall, at the time of providing the base services (specifically when opening the bank account), have to take action for the full identification of the customer and estimation of his anticipated level of activity as follows:

- Receiving a valid introduction letter signed by at least one of the recognized customers or the trusted persons or an introduction letter from one of the credit institutions licensed by the Central Bank of I.R.I., governmental organization and/ or official professional entities and associations.

- Obtaining information from the customer regarding his relationships with the designated persons involved and making inquiries from such persons to establish the authenticity of the information given by the customer.

- Receiving the valid businesses license especially with regards to the designated non- financial businesses and professionals which are more prone
to money laundering activities such as jewelers, dealers in precious metals/ stones, real estate and car dealership agencies.

andatory

- Obtaining the employment certificate from the natural persons who hold business licenses and/or the legal entities that hold national codes.

- Obtaining information about the type and scope of the customer's activity to estimate the customer's anticipated level of return in his area of activity.

**Initial identification of legal entities**

Pursuant to AML Executive By-law, The initial identification of a legal entity shall place on the basis of the national code and zip (postal) code of the legal entity's domicile and checking it/them with the original(s) or attested copy of identity card (as stated in the by-law requiring the use of national of legal entities).

With respect to the foreign legal entity, the identification shall take place by receiving the records of valid business license in Iran and the special number for aliens obtained from the National Database for Aliens.

The initial identification of a natural person introduced by a legal entity shall take place in accordance with the standards for natural persons.

The officers in charge of initial identification of customers shall, in the circumstances where any ambiguity exists as to the authenticity of the identification records delivered by customers, have to take action to lift ambiguity and verify customer's records through search in other databases and systems and/or make inquiries from the appropriate well-informed authorities. Nevertheless, the service provision shall be stopped until when the ambiguity has been clarified.

**Full identification of legal entities**

- Obtaining information about the type, nature scope of the customer's activity to estimate the anticipated level of activity.

- Obtaining information about articles of association, articles of incorporation, major shareholders, type of activity, providers of financial resources and their domiciles.
Obtaining information about the company compliance ratings from the appropriate authorities (such as rating agencies, ranking by the Vice-President's Office for Planning and Strategic Supervision and/or professional entities).

**Initial identification of non-banking issues**

According to AML Executive By-law, all persons who are change of providing services related to the safe deposit boxes and post boxes (mail boxes) in the country shall have to identify customers at the time of service provision. All persons who engage in accepting or handing deposits and providing postal services to customers shall have to identify customers in the circumstances where the applicable designated threshold.

All trades union/guilds which are prone to be abused by money launderers shall have to take action for initial identification of customers in all transaction above the applicable designated threshold and make entries. Such entities shall also have to record the unique number of persons in the sales invoices.

**Ongoing due diligence**

The designated persons providing base services shall have to continuously update the data relating to the full identification of customers, more specifically in the following circumstances:

a) When, based on the evidence and causes, there will be a probability that the customer's statement of account has undergone material changes;

b) Where the designated persons, based on the evidence and causes, sense a probability that the customer has been involved in money laundering operations and/or terrorist financing.

**Timing of verification**

The designated persons shall, at the time of providing the base services (specifically when opening the bank account), have to take action for the full identification of the customer and estimation of his anticipated level of activity.
Existing customers

Pursuant to Article 15, the designated persons have to perform the foregoing duties with respect to the former customers who used to benefit from the base services and, by the same token, are still carrying on their activities:

That group of the former customers whose particulars are found to have discrepancies at the matching stage shall have to remove the discrepancies within three months. If such discrepancies are not removed, the units of anti-money laundering in each establishment shall have report the matters to the financial intelligence unit.

That group of the former customers whose average size of activities in a year is insignificant as per the rules approved by the Council shall be excluded from the application of this article.

Politically exposed persons (PEP)

According to Article 9 of AML law, the designated persons shall have to exercise special care and control when opening and freezing the accounts for the politically exposed foreign persons.

3.3.1.3. Financial institution secrecy

U.K

The Financial Action Task Force (2007) reported that, there are no financial institution secrecy laws in the UK. MLRs Regulation 26(5) specifically provides that where a supervisory authority reports evidence of money laundering to the police then this is not taken to breach any restriction on the disclosure of information.

The FSA has comprehensive powers to require the production of information and documents from persons, including from persons outside of the regulated community. Its wide range of powers includes the power to compel, from any person, such information and documents as the investigator may require for the purposes of the investigation and also to attend before the investigator at a specified time and place to answer questions.
The FSA has adequate authority to share information when appropriate. Moreover, the confidentiality regime set up under the Financial Services and Markets Act 2000 (FSMA), includes a number of exceptions or “gateways” allowing the FSA to disclose to other UK bodies with financial crime interests information it has obtained, whether voluntarily or using compulsory powers.

According to the Financial Action Task Force (2007), there are no restrictions on the sharing of information between financial institutions. Regarding wire transfers, EC Regulation No 1781/2006 came into force in December 2006, and includes requirements for wire transfers to contain information on customer’s name, address and account number. The DPA implements the Data Protection Directive into UK law. One of its requirements is that all personal data processing be conducted fairly and lawfully. The DPA also imposes a restriction on transferring personal data outside the European Economic Area unless that state ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

U.S

According to the Financial Action Task Force (2006), the principal U.S statute protecting the confidentiality of financial information is the Right to Financial Privacy Act (RFPA). Generally, the RFPA governs both how U.S federal agencies obtain information from FIs and under what circumstances they may disclose such information. The overall purpose of the RFPA is to protect individuals who are customers of FIs from unwarranted intrusion into their records by the government. The Act makes it unlawful for a financial institution to release financial records of any individual customer or partnership of five or fewer individuals to the U.S Government, except in accordance with the provisions of the Act. The RFPA also provides for access to financial records through other mechanisms, including an administrative subpoena or judicial subpoena. The Section 314(b) of USA PATRIOT Act permits financial institutions, upon providing notice to the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity.
India

The rules as stipulated by the Reserve Bank of India Act state that banks, FIs and intermediaries are not allowed to disclose confidential information unless as stated by the RBI specifically. They must comply with disclosure requests by the RBI that include information such as “the persons to whom, and the purposes and periods for which, finance is provided.” This rule provides the RBI with the authority to call for information from bank and non-bank FIs and to give directions to the same. The RBI may also, at any time direct that every non-banking institution furnish to the Bank, in a manner and form it prescribes, those statements and other information or particulars relating to or connected with deposits that it holds. This includes those disclosures that have been determined to be in the public interest and in accordance with the law. Additionally, the PMLA states that the Central Government may prescribe the procedure and the manner of sharing information to the appropriate authorities, and that banking companies, financial institutions, intermediaries and their officers shall not be liable to any civil proceedings against them for furnishing this information.

Similarly, under the SEBI Act, the SEBI is authorized to call for any information from any of its stock exchanges, mutual funds, and other persons associated with securities market intermediaries and self-regulatory organizations. Additionally, they are able to access any information of publicly listed companies and share this information for financial investigation purposes.

Authorized money service businesses and exchange dealers are covered by similar disclosure requirements under section 11(2) of the FEMA empowers the RBI to direct any authorized person to furnish such information as the RBI deems fit.

Iran

All designated persons shall have to provide the information requested by the financial intelligence unit regarding the anti-money laundering activities in a manner established by such unit to perform the assigned duties (Article 47 of Executive by-Law).

According to Article 8 of AML law the documents and information which are collected in enforcement of this law shall be utilized merely towards the goals set
forth in the Anti-Money Laundering ACT and its predicate offences. The disclosure of information or use of it in one's own interest or for another party directly by the government officials or other persons designated in this law shall be prohibited and the offender shall be sentenced to the penalties prescribed in the law of the punishment for publication and Disclosure of the Governmental Confidential and Secret Documents enacted on Feb. 18th, 1975.

Moreover, according to Article 19, Regulations concerning prevention of Money Laundering through Financial Institutions, Members of the board, directors and/or employees of FIs are in no way allowed to disclose information related to suspicious activities of their applicants or customers to them or to third parties.

3.3.1.4 Record keeping

The purpose of keeping records is to enable law enforcement to reconstruct business transactions; often well after the original business has been concluded. Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity (FATF Recommendation 10). According to Basel Committee on Banking Supervision, banks should develop “clear standards on what records must be kept on customer identification and individual transactions and their retention period”. Pursuant to Wolfsberg AML Principles 9, bank will establish record retention requirements for all anti-money-laundering related documents. The documents must be kept for a minimum of five years.

U.K

According to MLRs Regulation, records on transactions must be kept for a period of 5 years from the date of the transaction. MLRs Regulation also require that evidence of identity for at least five years after the end of the end of the business relationship or five years after a one-off transaction has been completed. In order to comply with
other obligations solicitors may be required to retain files for a period of at least 6 years (Raphael, 2006). JMLSG Guidance and HMRC Guidance, MSB2, also deals with record keeping.

**U.S.**

The Banking sector, Securities sector and Insurance Sector must maintain a record of all identifying information about a customer, as well as noting the type of document, any identification number, the place and date of issue, and the expiration date of any document it used to obtain that information.

The record must also include a description of the method used to verify identity. Records of customer identification data collected under the CIP rules must be retained for a period of five years after the date on which the account is closed. With regard to the maintenance of records of correspondent accounts for foreign banks originals or copies of documents provided by the foreign bank must be retained for at least five years after account closure. A similar retention period is specified for any reports filed with FinCEN under the CTR and SAR requirements (Financial Action Task Force, 2006). There is a requirement that all such records required must be retained for a period of at least five years from the date of the transaction.

**India**

FIs covered under the Banking Regulation Act 1949, are obligated to prepare and maintain documentation on their customer relationships as well as transactions as specified by the RBI through directions they are authorized to deliver to the sector as they see fit.

Moreover, Section 12 of the PMLA, 2002 casts certain obligations on the banking companies in regard to preservation and reporting of customer account information. Banks are, therefore, advised to go through the provisions of PMLA, 2002 and the Rules notified there under and take all steps considered necessary to ensure compliance with the requirements of Section 12 of the Act ibid. Notification number 9/2005 dated 1st July, 2005 notifies rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for
furnishing of information and verification of records of the identity of the clients of the banking companies, FIs and intermediaries of securities market.

Banks should introduce a system of maintaining a proper record of transactions prescribed under Rule 3 of Notification number 9/2005 as mentioned below:

- all cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;
- all series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten Lakh;
- all cash transactions were 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 and
- all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules 3.

According to Notification number 9/2005, Rule 4, Banks are required to maintain the following information in respect of transactions:

- the nature of the transactions;
- the amount of the transaction and the currency in which it was denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction.

Such records and related documents should be made available to help auditors in their day-to-day work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities. These records are required to be preserved for ten years as is required under PMLA, 2002.

The Securities and Exchange Board of India (SEBI) has implemented similar provisions for record keeping of transactions and customer identification data.
Registered Intermediaries should ensure that all customer and transaction records and information are available on a timely basis to the competent investigating authorities. The following document retention terms should be observed:

(a) All necessary records on transactions, both domestic and international, should be maintained at least for the minimum period prescribed under the relevant Act (PMLA, 2002 as well SEBI Act, 1992) and other legislations, Regulations or exchange byelaws or circulars.

(b) Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence should also be kept for the same period (Guidelines for Anti-Money Laundering Measures).

According to Guidelines on Anti Money Laundering programme for Insurers, The insurer/agents/corporate agents are required to maintain the records of types of transactions mentioned under Rule 3 of PMLA Rules 2005 and the copies of the Cash/Suspicious Transactions reports submitted to FIU as well as those relating to the verification of identity of clients for a period of 10 years.

**Iran**

According to Article 33 of Executive By-Law, All designated persons shall have to maintain the documentation relating to financial transactions and operations (whether active or non-active) and also the documents relating to customer's identification data when providing the base services in the physical form and/or in other lawful methods for at least five years after the end of transactions. The settlement board of the legal entities involved shall, in case of the winding-up, have also to keep the documents up to five years after the financial events.

The records and documents shall be filed and kept in a manner that the information included in such documents can be accessed at the request of the financial intelligence unit and other appropriate authorities. The original documents and records, if requested by the financial intelligence unit and other appropriate authorities, shall have to be produced within one month at the latest. The designated person shall have the responsibility of search in and presentation of documents.
Moreover, the designated persons shall have to organize their financial and administrative structures in a manner that all accounts and records of a person be coherent, recognizable and verifiable (Article 34 of Executive by-Law).

3.3.1.5 Monitoring of transactions

Financial institutions should develop programmes against money laundering and terrorist financing. These programmes should include:

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

b) An ongoing employee training programme.

c) An audit functions to test the system (FATF Recommendation 15).

According to, Wolfsberg AML Principles “A sufficient monitoring program must be in place. The primary responsibility for monitoring account activities lies with the private banker. The private banker will be familiar with significant transactions and increased activity in the account and will be especially aware of unusual or suspicious activities (see 4.1). The bank will decide to what extent fulfillment of these responsibilities will need to be supported through the use of automated systems or other means.”

U.K

Financial Action Task Force (2007) reported that, the UK authorities derive from the requirements for monitoring though MLRs Regulation 3(1) (b); the reporting obligations under the POCA sections 330 and 331; the reporting obligations under section 21A of the TACT; and the FSA Handbook, SYSC 3.2.6 R that FIs will establish and maintain an appropriate approach to enable them to detect transactions and activity that may indicate money laundering or terrorist financing. So, there is no specific obligation to pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or
lawful purpose. However, JMLSG Guidance encourages financial institutions, in the context of the risk based approach and the requirements to have adequate systems and controls to combat ML, to have monitoring systems and provides examples of situations where staff should pay special attention and ask further questions.

The JMLSG Guidance states that FIs should monitor customer activity and Transactions. According to JMLSG Guidance and also HMRC Guidance, MSB2 Guidance, Records of all internal and external reports and letters from SOCA or any other correspondence with a law enforcement agency should be retained for at least five years from the date the report was made.

U.S

Banks, securities broker-dealers, futures commission merchants and introducing brokers in commodities are obligated under the BSA to file suspicious activity reports, and reports on a number of specified types of transactions (Financial Action Task Force, 2006).

According to the FFIEC Manual, FIs must have appropriate policies, procedures and processes in place to monitor and identify unusual activity, with particular emphasis on high-risk products, services, customers and geographic locations.

India

Banks should appoint a senior management officer to be designated as Principal Officer. The Principal Officer shall be located at the head/corporate office of the bank and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He will 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 Principal Officer will be responsible for timely submission of CTR, STR and reporting of counterfeit notes to FIU-IND.

Iran

According to Article 18 of Executive By - Law , the designated persons and also the board of directors of trades union of the designated non- financial businesses and
professions shall have to introduce a unit to be responsible for anti-money laundering activities to the SCS subject to their organizational scope and expansion. The secretariat may, if need be, verify the qualifications of the said unit members.

All designated persons shall, proportionate to the scope of their organizations, make the necessary arrangements in a manner to obtain the assurance required for the enforcement of the law and regulations governing the anti-money laundering activities.

At the time of certifying the qualifications of individuals, the SCS shall, in addition to their professional competence, have also to establish their general and security competence by making inquiries from the appropriate authorities.

The functions of individuals or responsible unit under article (18) are as follows:

a) To examine, prioritize and comment on the reports sent by the personnel of the appropriate authorities.

b) To promptly send such reports in the specified formats to the financial intelligence unit without the customer's knowledge. The time-limit for the "promptness" indicated in this article shall be notified in separate directives subject to the status of the designated persons. This period, shall not, however, exceed four business days.

c) To monitor the activities of the clients using the base services to identify the suspicious transactions.

d) To prepare the necessary software to facilitate quick access to the required information in enforcing the laws and regulations and accordingly in the systemic identification of suspicious transactions.

e) To devise the required mechanism to control the anti-money laundering processes (the process of collecting and analyzing information, recruitment of staff, training and the like) and assess and evaluate its compliance level in the appropriate establishments.

f) To provide supplementary information required by the financial intelligence unit and other authorities which are competent in the fight against terrorism.
g) To issue the required circulars as the execution of the law and regulations governing the anti-money laundering operations upon the agreement of the SCS.

h) to conduct inspection of the subordinate to ensure the strict observance of laws and regulations.

i) to prepare the statistics relating to the measures carried out by the appropriate establishment in the anti-money laundering and the outcomes thereof.

J) to send the records of the persons stated in note (3) of article (4) of law to the appropriate authorities in coordination with the financial intelligence unit.

k) to keep the records and reports of correspondence relating to the appropriate establishment concerning the issues of money laundering and terrorist financing.

l) to draft the annual program for law enforcement by the designated persons and monthly control of the level of its compliance.

3.3.1.6 Suspicious transaction reports

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the FIU (FATF Recommendation 13).

According to Wolfsberg AML Principles, private banker, management and/or the control function will carry out an analysis of the background of any unusual or suspicious activity. If there is no plausible explanation a decision will be made involving the control function:

- To continue the business relationship with increased monitoring
- To cancel the business relationship
- To report the business relationship to the authorities.

U.K

The legal obligation on the regulated sector to submit suspicious activity reports is set out in POCA. POCA makes it an offence for someone working in the regulated sector
that knows or suspects or has reasonable grounds for knowing or suspecting that
another person is engaged in money laundering, not to disclose this either to their
institution’s “nominated officer” or directly to the UK FIU. Where firms have the
opportunity to delay or stop a transaction they suspect of being involved in ML/TF,
they must do so and seek consent from the UK FIU. The FIU then has seven days to
determine whether or not to grant consent for the transaction to continue. Where the
amount under consideration is less than £250, there is not an automatic duty to seek
consent.

U.S

FinCEN has issued federal regulations implementing 31USC 5318(g) that require a
broad range of FIs to report suspicious transactions relating to both money laundering
and terrorist financing. These regulations apply to banks, securities broker-dealers,
MSBs, except check cashers, futures commission merchants and introducing brokers
in commodities and insurance companies.

India

Section 12(1) (b) of the PMLA requires covered FIs to report to the FIU such
transactions as may be prescribed. Prescribed transactions are defined in the Rules as
cash transactions (including multiple linked transactions) in excess of Rs.1million
(US$45,000), cash transactions involving counterfeit currency, and suspicious
transactions (whether in cash or otherwise) performed through a specified list of
payment instruments within a defined range of different business relationships.

In terms of the PMLA rules, banks are required to report information relating to cash
and suspicious transactions to the Director, FIU-IND in respect of transactions
referred to in Rule 3.

Banks should make STRs if they have reasonable ground to believe that the
transaction involve proceeds of crime generally irrespective of the amount of
transaction and/or the threshold limit envisaged for predicate offences in part B of
Schedule of PMLA, 2002 . The Suspicious Transaction Report (STR) should be
furnished within 7 days of arriving at a conclusion that any transaction, whether cash
or non-cash, or a series of transactions integrally connected are of suspicious nature.
The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. Banks should not put any restrictions on operations in the accounts where an STR has been made. Moreover, it should be ensured that there is no tipping off to the customer at any level.

Insurance companies also should report the suspicious transactions immediately on identification. When such transactions are identified post facto the contract, a statement may be submitted to FIU-IND within 3 working days of identification in the prescribed formats.

**Iran**

According to Article 25 of Executive by-Law of the Anti-Money Laundering ACT, all the staff working under the designated persons shall, in case of observing the suspicious transactions and operations have to report the matter to the anti-money laundering units of each establishment without the client's knowledge. If such unit does not exist, the highest official of the designated persons shall bear the responsibility of receiving reports and taking appropriate measures. If the customer informed of such matter, the violator shall be treated in accordance with the prevalent rules.

The staff working under the designated persons shall have to enter all the transaction above the applicable designated threshold for which the customer pay in cash and report the matter along with the customer's explanations to the anti-money laundering units in each establishment and, where such unit does not exist, to the highest official of the designated person. the anti-money laundering units in each establishment and/or the highest official of the designated person (where such unit does not exist) shall, at end of each week, have to submit a summary of the said forms in the manner indicated by the financial intelligence unit and keep the originals in strict safeguards (Article26 of Executive by-Law of the Anti-Money Laundering ACT).

Money remitters above of applicable designated threshold shall have to give the explanations required in the declared forms to the designated persons. In the case of cash transfer above the applicable designated threshold by using non-banking practices such as by post/mail, the staff of the designated persons shall have to report
the matter to the anti-money-laundering units in each establishment. Where such unit
does not exist, reports shall have to be addressed to the highest official of the
designated person to adopt appropriate measures.

Pursuant to Article 27 of Executive by-Law of the Anti-Money Laundering ACT, the
report on the suspicious transactions and accordingly the reports which the designated
persons are bound to send shall imply no accusation whatsoever against individuals
and the reporting of such transaction to the financial intelligence unit shall not be
considered disclosure of personal secrets and, as a result, no charge whatsoever shall
be leveled against the reporters when enforcing the present by-law.

3.3.1.7 Internal controls, compliance, audit and foreign branches

U.K

According to the MLR 3 and 7, FIs have to implement appropriate internal controls in
order to comply with their AML/CFT obligations. MLRs Regulation also requires FIs
to make their staff aware of the provisions, and to provide training on how to
recognize and deal with transactions which may be related to money laundering.
Failure to take these steps leaves the firm open to prosecution for having inadequate
training and awareness arrangements. Individual members of staff face criminal
penalties if they are involved in money laundering or terrorist financing or if they do
not report their knowledge or suspicion of money laundering or terrorist financing
where there are reasonable grounds for their knowing or suspecting such activity.

The format of the HMRC MSB2 Guidance is constructed around the mnemonic
CATCH, focusing on internal controls (FATF, 2007):

Control your business by having anti-money laundering systems in place

- Appoint a nominated officer
- Train your staff
- Confirm the identity of your customers
- Hold all records for at least 5 years
Pursuant to the MLRs FIs have to appoint a 'nominated officer' who is responsible for receiving internal money laundering disclosures and making external reports to SOCA where appropriate. The FSA requires the Money Laundering Reporting Officer (MLRO) to have a sufficient level of seniority within the financial institution to enable him to carry out his function effectively. The MLRO must have the authority to act independently in carrying out his responsibilities.

For independent audit function, FSA Handbook requires that a firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business. In relation to screening procedures, FIs have to operate adequate employee vetting procedures when recruiting certain new staff.

U.S

According to section 352 of the USA PATRIOT Act FIs must establish AML Programs, including, at a minimum: (1) the development of internal policies, procedures and controls; (2) the designation of a compliance officer; (3) an ongoing employee training program and (4) an independent compliance function to test programs.

As a result, the bank’s board of directors must designate a qualified employee to serve as the BSA compliance officer. The BSA compliance officer is responsible for coordinating and monitoring day-to-day BSA/AML compliance. The BSA compliance officer is also charged with managing all aspects of the BSA/AML compliance program and with managing the bank’s adherence to the BSA and its implementing regulations; however, the board of directors is ultimately responsible for the bank’s BSA/AML compliance (FATF, 2006).

Banks also, must ensure that appropriate personnel are trained in applicable aspects of the BSA. Training should include regulatory requirements and the bank’s internal BSA/AML policies, procedures, and processes. In respect to employee screening, they are strongly encouraged by the federal regulators to use reasonable employment screening processes to minimize the risk of fraud, embezzlement, money laundering, and other crimes.
India

The Reserve Bank of India guidelines issued in November, 2004 requires banks and other FIs supervised by the RBI to implement effective AML procedures.

The PMLA provide very limited direction to covered institutions with respect to internal procedures, policies and controls. These relate only to the implementation of a client identification programme, certain recordkeeping requirements, the procedures for supplying information to the FIU, and the appointment of a designated person to act as the money laundering reporting officer. The defined role of the principal officer is far narrower than that of a money-laundering compliance officer and relates only to the transmission of reports to the FIU (Asia/Pacific Group on Money Laundering, 2005).

Iran

Article 31 of Executive by- Law of the Anti- Money Laundering ACT stated that, all designated persons shall, by adopting the necessary measures, have to ensure that the anti-money- laundering regulations are observed in branches and agencies outside the country. Moreover, according to Article 32 of Executive by- Law the designated persons shall have to exercise the utmost caution in their transactions/exchanges with other countries and regions indicated by the council.

3.3.1.8. Shell banks

According to recommendation 18 of FATF, countries should not approve the establishment or accept the continued operation of shell banks. Also, FIs should not be permitted to enter into, or continue, correspondent banking relationships with shell banks. According to Basel Committee on Banking Supervision (2003), Shell banks are banks that have no physical presence in the country where they are incorporated and licensed, and are not affiliated to any financial services group that is subject to effective consolidated supervision. The mind and management are located in another jurisdiction, often located in the offices of an associated entity or sometimes in a private residence. According to Wolfsberg AML Principles for Correspondent
Banking, Shell banks are high risk banks principally due to the difficulty in monitoring and operating with great secrecy. Shell banks are a gateway for money launderers to carry out their actions in the financial system. So, an institution will not offer its products or services to a Shell Bank.

**U.K**

Pursuant to the money laundering regulation 2007, A “shell bank” means a credit institution, or an institution engaged in equivalent activities, incorporated in a jurisdiction in which it has no physical presence involving meaningful decision-making and management, and which is not part of a financial conglomerate or third-country financial conglomerate”.

Shell banks are not permitted to establish or continue to operate in the UK. The FSA’s authorization process helps to ensure that shell banks do not operate in the UK. All applications to carry out FSMA-regulated activities must be submitted to the FSA for approval, and the FSA will only authorize FIs if it is satisfied that they meet and will continue to meet the “threshold conditions.”

According to the JMLSG Guidance correspondents must not maintain relationships with shell banks and that Correspondent banks must not maintain relationships with shell banks nor any respondent which itself provides banking services to shell banks.

**U.S**

The establishment of shell banks is not permitted in the U.S, either at federal or state level. The BSA was amended by section 313 of the USA PATRIOT Act to prohibit U.S. FIs from establishing, maintaining, administering or managing a correspondent account in the U.S. for any foreign shell bank.

FIs must take reasonable steps to ensure that correspondent accounts provided to foreign banks are not being used to provide banking services indirectly to foreign shell banks. A financial institution is required to terminate immediately any account that it knows to be the account of a foreign shell bank or that it knows is being used indirectly by a foreign shell bank.
**India**

Shell banks are not permitted to operate in India. 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). Banks should also guard against establishing relationships with respondent foreign FIs that permit their accounts to be used by shell banks. Banks should be extremely cautious while continuing relationships with respondent 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.

**Iran**

According to Article 10 of Executive by- Law of the Anti- Money Laundering ACT, regulations concerning prevention of Money Laundering through Financial Institutions, opening accounts or rendering other banking services to unauthorized institutions or credit establishments are prohibited. Financial Institutions, which are subject to these Regulations, shall close the accounts of said institutions and cease to provide banking services to them, within the time limit determined by Central Bank of Iran. The name and identifications of the said institutions or establishments would be notified by Central Bank of the Islamic Republic of Iran.

**3.3.1.9 The supervisory and oversight system**

According to Recommendation 23, Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in a financial institution.
Supervisors have a duty not only to ensure their banks maintain high KYC standards to protect their own safety and soundness but also to protect the integrity of their national banking system. Supervisors around the world should seek, to the best of their efforts, to develop and implement their national KYC standards fully in line with international standards so as to avoid potential regulatory arbitrage and safeguard the integrity of domestic and international banking systems (Basel Committee on Banking Supervision - Customer due diligence).

**U.K**

Raphael (2006) stated that, the Financial Services Authority (FSA) is the UK’s single financial services regulator. It is an independent non-governmental body, given statutory powers by the Financial Services and Markets Act 2000. FSA established as a company limited by guarantee. The FSA has four regulatory objectives which are: market confidence, public awareness, the protection of consumers and the reduction of financial crime. The FSA's primary focus and activities are designed to ensure that the FIs it regulates have adequate systems and controls including in relation to preventing financial crime, which includes AML and CFT.\(^{21}\)

The FSA adequately funded, staffed and has sufficient technical and other resources to fully and effectively perform its functions. The FSA is accountable to Treasury Ministers and through them to Parliament. It is operationally independent of the Government. The FSA’s power to authorize and take enforcement action against FIs is independent of any involvement or influence from the UK Government. The FSA does not receive any funding from the Government. FSA staff is provided with adequate and relevant training to combat ML and TF. A number of areas within the FSA are involved in AML/CTF for example:

**Supervision:** The FSA’s supervisory areas are responsible for the day to day relationship with the FIs regulated by the FSA.

**Enforcement:** The Enforcement Division is responsible for investigating cases, including AML/CFT issues.

**Financial Crime Policy Unit (FCPU):** The FCPU leads the FSA’s development of anti-money laundering and fraud policy.
The FSA has a broad range of sanctions available to it against FIs and approved persons including unlimited financial penalties, public censure, prohibition, variation or cancellation of permission, injunction, issuance of a formal caution and prosecution for breaches of the MLRs. It also has enforcement powers that can be used against persons outside of the regulated community, such as the power to gather information and documents and the power to apply to court for injunctions.

U.S

The administration of the regulatory regime under the BSA is a core responsibility for FinCEN. Under the BSA, FinCEN has the authority to:

- investigate alleged violations;
- issue letters of caution or warning letters;
- seek injunctions;
- impose civil money penalties; and
- refer apparent criminal violations to the Department of Justice (DOJ).

Its regulatory functions are administered by the Regulatory Policy and Programs Division, which consists of three offices:

- The Office of Regulatory Policy is committed to administer effectively the BSA through the development and implementation of policy via outreach, training, and the issuance of regulations and guidance.
- The Office of Compliance works to help ensure industry compliance with the BSA through supporting and working in partnership with the agencies and organizations directly examining FIs for compliance.
- The Office of Enforcement seeks to sanction violations committed by financial institutions, obtain corrective action and deter future non-compliance.

In order to leverage existing examination resources and avoid unnecessary duplication of compliance inspections, FinCEN has formally delegated its authority to examine
FIs for compliance with the BSA to federal functional and financial regulatory agencies. These agencies comprise:

The Federal Deposit Insurance Corporation (FDIC), The FDIC directly examines and supervises more than 4,900 banks and savings banks for operational safety and soundness, more than half of the institutions in the banking system. The FDIC is the primary federal regulator of banks that are chartered by the states that do not join the Federal Reserve System. In addition, the FDIC is the back-up supervisor for the remaining insured banks and thrift institutions.

The Office of the Comptroller of the Currency (OCC), The Office of the Comptroller of the Currency (OCC) charters, regulates, and supervises all national banks. It also supervises the federal branches and agencies of foreign banks. Headquartered in Washington, D.C., the OCC has four district offices plus an office in London to supervise the international activities of national banks.

The Small Business/Self-Employed (IRS-SBSE), The mission of the Small Business/Self-Employed (SB/SE) Division is to provide SB/SE customers top-quality service by educating and informing them of their tax obligations, developing educational products and services, and helping them understand and comply with applicable laws, and to protect the public interest by applying the tax law with integrity and fairness to all.

The Office of thrift supervision (OTS), The Office of thrift supervision (OTS) supervises a national thrift industry that is built on the bedrock of the American dream of homeownership—supplying affordable home financing for Americans from all walks of life.

The National Credit Union Administration (NCUA), The National Credit Union Administration (NCUA) is the independent federal agency that charters and supervises federal credit unions. NCUA, backed of the full faith and credit of the U.S. government, operates the National Credit Union Share Insurance Fund (NCUSIF) insuring the savings of 80 million account holders in all federal credit unions and many state-chartered credit unions.
Securities and Exchange Commission (SEC), the mission of the U.S. Securities and Exchange Commission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation.

The Commodity Futures Trading Commission (CFTC), Congress created the Commodity Futures Trading Commission (CFTC) in 1974 as an independent agency with the mandate to regulate commodity futures and option markets in the United States. The CFTC's mission is to protect market users and the public from fraud, manipulation, and abusive practices related to the sale of commodity and financial futures and options, and to foster open, competitive, and financially sound futures and option markets.

**India**

There are three primary financial services regulators in India: the Reserve Bank of India, the Securities and Exchange Board of India and the Insurance Regulatory and Development Authority.

The RBI has a well developed system of supervision based around licensing requirements and a combination of offsite surveillance and onsite inspection. All FIs defined within the Banking Regulation Act and the RBI Act requires a licence from the RBI. The SEBI has similar licensing and oversight powers and responsibilities to those of the RBI, although it has the authority to delegate some of its rule-making and compliance functions to the 24 exchanges, which are deemed to be self-regulatory organizations (section 19 of the SEBI Act). The IRDA has similarly extensive powers to those of the RBI and the SEBI (section 14 of the IRDA Act).

**Iran**

The regulatory or supervisory authorities monitoring the designated persons (such as the central bank of Iran, Central Insurance Corporation of Iran, Securities and Exchange Organization, the State Inspectorate General Organization, the State Organization of Lands and Deeds Registration, Trades Union/Guilds, Organization of Endowment and Charity Affairs) shall, in their normal inspection tours, have to take account of the rules for combating money laundering and terrorist financing and
comment on the compliance or non-compliance with such rules (Article 20 of Executive by- Law of the Anti- Money Laundering ACT).

The SCS shall have to examine the performance of the authorities referred to in article (20) once every six months and report the matter to the council.

### 3.3.1.10 Money or value transfer services

A value transfer system refers to any system, mechanism, or network of people that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, whether or not in the same form. A value transfer system may fall into one or more of these groups: Informal Value Transfer Systems (IVTS), Retail value transfer systems and Institutional formal value transfer systems. The most important IVTS identified so far are: Hawala, Hundi, Black market peso exchange networks, Fei chien, door-to-door, and other Asian varieties, Invoice manipulation schemes, In-kind fund transfers (India and elsewhere) etc (Nikos Passas, 2003).

**U.K**

According to MLRs Regulation Money value transfer services (MVTs) fall within the money service businesses category. This category includes “traditional” MVT operators such as Western Union and also alternative remittance business since the regulations merely refer to the activity being conducted. HMRC holds a register of all MSBs, broken down by category. MVTs are separately identifiable within the register. MVT operators as MSBs are covered by the rules of the MLRs. So, MVT service providers are “MSBs” in the UK; they are registered and supervised by the HMRC for AML/CFT regulation.

**U.S**

Money or value transfer services provided in the U.S. by non-bank FIs are included in the category of money services businesses. Under U.S. law, all money transfer services, both formal and informal systems, are considered money services businesses (MSBs) under the law, and are subject to any BSA requirement applicable to any
Money transmitter, including registration as an MSB with FinCEN, the establishment of an AML Program, appropriate record keeping, and the reporting of suspicious activity.

**India**

Money services businesses and foreign exchange houses are licensed by the RBI under the Foreign Exchange Management Act (FEMA) which replaced the Foreign Exchange Regulation Act (FERA). The primary enforcement authorities overseeing this sector are the Department of Revenue Intelligence and the Enforcement Directorate within the Ministry of Finance. Money service businesses and Exchange dealers are considered “authorized persons” once licensed by the RBI to send and receive payments from overseas and to hold foreign exchange. These businesses are subject to transaction reporting requirements that include every fourteen days for foreign exchange houses (of all sales transactions regardless of amount), and once a month for ‘authorized money changers’ (AMCs). They are also obligated to submit suspicious transaction reports and large currency transaction reports directly to the RBI.

**Iran**

According to Article 28 of Executive By-Law, the purchase and sale of Foreign currencies in any manner including the payment of local currency (rials) inside the country and receipt of Foreign currency outside the country and vice versa shall be authorized only through the banking systems and licensed exchange offices pursuant to the laws and regulations in force. Failing to do so, the buying and selling of foreign currencies shall be deemed to be unauthorized and, in a such case, the provisions of the law on the Procedures of Imposing state Penalties Regarding the Commodity and foreign Currency Smuggle approved in 1995 by the Expediency Council shall prevail.

The Central bank of I.R.I. at the end of each day, have to enter the detailed information concerning the purchase, sale and transfer of foreign currencies through the banking system and licensed exchange offices in the databank which has been organized for such purpose and further shall provide the opportunity of access to and search in it by the financial intelligence units (Article 29 of Executive By-Law).
3.3.2 Designated Non – Financial Businesses and Professions

According to FATF designated non-financial businesses and professions (DNFBPs) include:

- Casinos (which also includes internet casinos).
- Real estate agents.
- Dealers in precious metals.
- Dealers in precious stones.
- Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to ‘internal’ professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.
- Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:
  - acting as a formation agent of legal persons;
  - acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
  - providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
  - acting as (or arranging for another person to act as) a trustee of an express trust;
  - acting as (or arranging for another person to act as) a nominee shareholder for another person.
Recommendations 5-16 and 21-22 of FATF state that designated non-financial businesses and professions should take certain actions. These references require countries to take measures that will oblige FIs or designated non-financial businesses and professions to comply with each Recommendation. The basic obligations under Recommendations 5, 10 and 13 should be set out in law or regulation, while more detailed elements in those Recommendations, as well as obligations under other Recommendations, could be required either by law or regulation or by other enforceable means issued by a competent authority.

3.3.2.1 Customer due diligence and record-keeping

U.K

Casinos: MLRs Regulation 8 explicitly requires that casino operators to obtain satisfactory evidence of identity of any person before allowing that person to use the casino's facilities. Moreover, the Gambling Commission has issued guidance entitled: “Guidance to the Operators of Casinos for the Purposes of Preventing and Detecting Money Laundering”. The guidance covers the following areas: knowing your customer; recording identification; retention of identification records; recording transactions; retention of transaction records; reporting systems for suspicious activity; identifying suspicious transactions; training and compliance; and confidentiality. Gambling Commission Guidance recommends that casinos keep transaction records in relation to cash transactions, cheques, bank drafts, and deposits. The guidance also states that transaction records must be retained for at least 5 years from the date of the transaction.

Real Estate Agents: Real estate agents would need to conduct CDD if and when they establish business relations, conduct a one-off transaction above 15,000 euros, or where money laundering or terrorist financing is suspected. The Royal Institute of Chartered Surveyors produces guidance on AML/CFT legislation for its members entitled “protecting against money laundering: a guide for members”. 22

Dealers in precious metals & dealers in precious stones: Dealers in precious metals & dealers in precious stones fall into the wider category applicable in the UK, that of
“high value dealers” (HVDs), which is adequately covered under the regulations by requiring CDD when conducting any one-off transaction over 15,000 euros.

HMRC has issued a sector-specific guidance entitled: “Anti money laundering guide for High Value Dealers”. This notice explains the: Primary law relating to money laundering; and Money Laundering Regulations 2003 and their effect on businesses accepting payment in cash equivalent to 15,000 or more euros for goods.

HMRC Guidance for HVDs advises: “… You should regularly review the relationship and consider reporting any suspicion. You must retain the account file or an equivalent record for five years after you stop dealing with the customer…you need not establish any additional records, provided your commercial files meet the requirements of the regulations and you are able to produce them when required to do so”.

Lawyers: The MLRs covers lawyers. The guidance produced by the Law Society of England and Wales sets out the general rationale for AML compliance requirements, namely: to enable suspicious transactions to be recognized and reported to the authorities; and to ensure that the audit trail is available if a solicitor, client or other party to a transaction becomes the subject of an investigation (Raphael, 2006). Guidance by the Bar Council England & Wales suggests that barristers should comply with the record-keeping requirements as follows:

- As regards evidence of client identity, if a barrister has obtained this himself, he must retain the records for 5 years
- If the barrister has asked an instructing professional to certify that customer due diligence checks have been carried out:
  - the barrister will ask the instructing professional to certify that the instructing professional has proper record-keeping measures in place to comply with Regulation 6 of the Money Laundering Regulations 2003: with the result that the barrister can subsequently request the instructing professional to produce the evidence of client identity if the need to do so arises; (ii) barristers in Northern Ireland will apply the same approach as in (i) above, but in addition are required to retain the certification for 5 years.
As regards evidence of the transaction itself, if a barrister has been instructed by another regulated professional, he will ask that professional to confirm in writing that the instructions and advice will be kept by the professional for the requisite period.

Licensed conveyancers: A Licensed Conveyancer is a specialist legal professional in the UK who has been trained to deal with all aspects of property law. Statutory regulator the “Council for Licensed Conveyancers” (CLC) has produced guidance specific to these specialist property lawyers.24 According to the CLC guidance “Records of customer identification and KYC transaction assessments must be made and retained for use as evidence in any subsequent investigation into money laundering… Prudence suggests that they should also be capable of identifying all internal suspicion reports received and all external reports made”.

Accountants: Accountants, auditors or tax advisers are required to comply with the customer due diligence, record keeping and other requirements of the MLRs for all their business activities. In addition to the legal obligations, accountants are informed in their CDD activity by guidance produced by the Consultative Committee of Accountancy Bodies (CCAB). The CCAB Guidance states that evidence of client identification needs to be maintained for five years after the termination of a client relationship by any part of the firm providing relevant business. Records of transactions also need to be maintained for five years, from the date when all activities in relation to the transaction were completed (Raphael, 2006) and (Greenfield, 2004).

Trust & Company Service Providers (TCSPs): Trust and company service providers are subject to the ML regulations when commencing a business relationship, conducting a one-off transaction over 15,000 euros, or when suspecting money laundering or terrorist financing.

U.S

Casinos: Casinos are subject to the following BSA requirements:

- Suspicious transaction reporting;
Reporting of transactions in currency;

Record keeping;

Establishing AML Programs.

Gaming establishments with gross annual revenue of USD 1 million or less are not subject to these requirements. The BSA does not permit casinos to keep anonymous accounts or accounts in fictitious names involving deposits and credits. However, casinos are required to collect and verify customer identification information when there is:

- a deposit of funds, account opened or line of credit extended.
- a transaction for or through a customer's deposit or credit account.
- an extension of credit in excess of USD 2,500.
- an advice, request or instruction with respect to a transaction involving persons, accounts or places outside the U.S., regardless of residency.
- a transaction with a face value of USD 3,000 or more.
- transmittals of funds in excess of USD 3,000.

Casinos are required to maintain and retain the original or a copy of certain records for a period of five years.

Accountants: Accountants are not defined as “financial institutions” under the BSA, and accordingly they are not currently subject to most of the AML requirements under the BSA. Accountants have no customer identification obligations. Accountants are required to maintain the information collected for the purpose of meeting their reporting requirements for five years.

Dealers in precious metals and stones: Although a dealer in “precious metals, stones, or jewels” defined as a financial institution under the BSA, FinCEN had not previously defined the term or issued regulations regarding the dealers. Dealers in precious metals and stones have no customer identification obligations. Dealers in
precious metals and stones are required to maintain the information collected for the purpose of meeting their reporting requirements for five years.

Lawyers: Lawyers and other legal professionals in the U.S. are not defined as “financial institutions” under the BSA and are not currently subject to most of the AML requirements. Lawyers have no customer identification obligations. Lawyers are required to maintain the information collected for the purpose of meeting their reporting requirements for five years.

Real estate agents: The BSA defines “persons involved in real estate closings and settlements” as a type of financial institution. The U.S. recognizes that the real estate industry and persons involved in the industry could be vulnerable to money laundering and other financial crime but the U.S. has not yet adopted a final rule relating to such persons. Real estate agents have no customer identification obligations. Real estate agents are required to maintain the information collected for the purpose of meeting their reporting requirements for five years.

Trust and company service providers: Trust companies that are authorized to act in a fiduciary capacity are defined as FIs under the BSA. They are chartered and regulated at either federal or state level, on a basis similar to that for banks, and are mostly subject to the same AML. The business of acting as an agent in the formation and administration of companies is not similarly defined, and so such businesses are not currently subject to AML requirements. Trust and company service providers have no customer identification obligations. Trust and company service providers are required to maintain the information collected for the purpose of meeting their reporting requirements for five years.

India

DNFBPs conducting business in India include casinos, lawyers, real estate agents, accountants, company secretaries, gold dealers, and dealers in precious metals and stones. There is no free-standing profession of trust and company service providers, but these services are provided by the other professionals, especially accountants and company secretaries. With the exception of casinos (which only operate in the State of Goa, and which were brought under the PMLA with effect from 1 June 2009), these
businesses are not subject to the PMLA provisions. However, some guidelines that have relevance to AML/CFT have been drawn up by the industry and professional bodies (FATF, 2010). With the introduction of the amendments to the PMLA in June, 2009, casinos were included within the definition of financial institutions. As a result, all the provisions of the PMLA and the accompanying Rules became applicable to this sector. However, casinos do not constitute FIs in the context of the RBI circulars, which, therefore, have no relevance to the casino sector.

Iran

According to Executive By- Law of the Anti- Money Laundering ACT, DNFBPs means the persons (natural/ legal) that engage in cash transitions with a high frequency and are prone to risks in terms of money laundering such as forward dealers in real estates and cars, jewelers dealers in valuable cars and carpets and dealers in antiques and precious cultural products.

The designated persons shall, at the time of providing base services to the DNFBPs, have to obtain the required obligation from them regarding the enforcement of anti-money laundering law and regulation whilst receiving the documents and records. In case of failure by the designated non- financial businesses of their obligations, the designated persons shall refuse to provide services to them (Article 7 of Executive By- Law).

Pursuant to Article 18 of Executive by- Law, the board of directors of trades union of the DNFBPs shall have to introduce a unit to be responsible for anti- money laundering activities to the SCS subject to their organizational scope and expansion. The SCS may, if need be, verify the qualifications of the said unit members.

All DNFBPs shall, proportionate to the scope of their organizations, make the necessary arrangements in a manner to obtain the assurance required for the enforcement of the law and regulations governing the anti- money laundering activities.

Moreover, all designated persons shall, when issuing licenses or extending the previous license for the DNFBPs in various sectors, have to obtain the appropriate obligation from applicants for the enforcement of the law and by-laws thereof
governing anti-money laundering and terrorist financing and shall keep them in their files. Inclusion of such obligations in the articles of association of legal entities may accordingly be mandatory in the circumstances indicated by the council (Article 45 Executive By- Law).

According to Article 3 of Executive By- Law of the Anti- Money Laundering Act, all designated persons shall have to make the initial identification of their customers at the time of performing any operations as well as providing services above the applicable designated threshold and/ or when suspicion is aroused in respect of money laundering activities. In the event that the customer does not produce the records and documents or suspicion exists as regards the money laundering activities or other related offences, the DNFBPs shall have to avoid providing services to them and shall report the matter to the finance intelligence unit.

3.3.2.2 Suspicious transaction reporting

U.K

The reporting requirements that apply to FIs under MLRs Regulation 7 and the obligations to report suspicious activity under POCA Sections 330-331, and TACT 21A, apply to DNFBPs; as do the accompanying safe harbor from liability & tipping off provisions. DNFBPs are required to report to the FIU when they suspect or have reasonable grounds to suspect that funds are the proceeds of all criminal acts that would constitute a predicate offence for money laundering domestically. The various DNFBPs are well aware of their reporting obligations and seem to have effective systems in place to comply with them. The limited exemption from the requirement to report money laundering does not extend to all accountants, auditors and tax advisers. It applies only to those who are members of a professional body which requires a test of competence as a condition of membership and the maintenance of professional standards, including sanctions for non-compliance with those standards (FATF, 2007).
U.S

A casino must have procedures for filing a report of any activity when there is a suspicion of money laundering or terrorist financing at the required reporting threshold. This suspicious activity reporting obligation applies to all casinos and card clubs with gross annual gaming revenues of USD 1,000,000 or more. Casinos must file a report of any suspicious transaction that it believes is relevant to the possible violation of any law or regulation that is conducted or attempted by, at, or through a casino, and involves or aggregates at least USD 5,000 in funds or other assets.

Accountants, dealers in precious metals and stones, lawyers, real estate agents and TCSPs are not required at this time to file SARs. They are permitted to report suspicious transactions voluntarily.

India

DNFBPs with the exception of casinos are not covered under the PMLA nor are they obligated to report any suspicious transactions to a competent authority (FIU). As regards the other DNFBP sectors, it is important that the Government extend the PMLA to the businesses and professions as soon as possible.

There seem to be some customer due diligence and record keeping obligations for gold dealers, as importers and authorized purchasers are registered and under supervision of the RBI.

Iran

According to Executive by- Law suspicious transactions and operations means the transactions and operations that persons, based on the availability of and information and/or the reasonable grounds mean the laundering activities.

All the staff working under the DNFBPs shall, in case of observing the suspicious transactions have to report the matter to the anti-money laundering units of each establishment without the client's knowledge. If such a unit does not exist, the highest official of the designated persons shall bear the responsibility of receiving reports and taking appropriate measures. If the customer is informed of such a matter, the violator
shall be treated in accordance with the prevalent rules (Article 25 of Executive by-Law).

3.3.2.3 Regulation, Supervision, and monitoring

U.K

Casinos: All casinos must be licensed under the Gaming Act 1968. The Gambling Commission is a regulatory body with powers of monitoring and sanctions under the Gaming Act 1968 and from September, 2007 the Gambling Act 2005. In accordance with its statutory objective to prevent the exploitation of gambling for financial crime, it is explicitly tasked with supervising casinos for compliance with the AML/CFT controls, including the legal obligations under MLRs, POCA, and TACT, and the additional obligations imposed by its own guidance in this regard. It can apply its own regulatory sanctions if it determines that a casino has failed to apply sufficient AML/CFT controls; but for criminal prosecution under MLRs, POCA, or TACT, it refers cases to the police.

Real estate agents: The Royal Institute of Chartered Surveyors (RICS), the professional body, produces guidance and news bulletins on AML/CFT legislation and developments for its members on its website. It has also worked with trade bodies like the National Association of Estate Agents to produce guidance “Protecting against money laundering: a guide for members”.

High Value Dealers: HMRC is the statutory supervisor of HVDs, including dealers in precious metals and stones. HMRC has powers under the MLRs to: require further information related to the registration; determine an application to register; cancel a registration; set and charge fees; inspect premises; inspect and copy records; where a Justice is satisfied that a regulatory offence may be being committed: obtain access orders for recorded information and obtain a search; impose civil penalties of up to £5,000 for regulatory breaches; and prosecute regulatory breaches.
Solicitors: The Law Society England & Wales, Law Society of Scotland and Law Society Northern Ireland are a supervisory authority in accordance with the Money Laundering Regulations.

Barristers/Advocates: The practice of barristers in England and Wales and Northern Ireland is supervised by the Bar Council England and Wales (BCEW) and the Bar Council Northern Ireland (BCNI), respectively, which would consider failure to comply with the provisions of the Money Laundering Regulations, the POCA, or the TACT to be professional misconduct.

Licensed Conveyancers: The statutory registrar and regulator of licensed Conveyancers is the Council for Licensed Conveyancers (CLC) which supervises its members for compliance with the relevant professional standards and for compliance with AML/CFT controls. The CLC’s “Discipline and Appeals Committee” has statutory sanctions that include the power to levy fines on licensed Conveyancers and the power to withdraw licenses to operate; these sanctions can be applied in circumstances where the conveyancer has failed to abide by AML/CFT controls.

Accountants: The following bodies (the 4 accountancy supervisory bodies) are “supervisory authorities”:

- The Institute of Chartered Accountants in England & Wales;
- The Institute of Chartered Accountants in Ireland;
- The Institute of Chartered Accountants of Scotland;
- The Association of Chartered Certified Accountants.

U.S

Casinos: In the U.S., gambling regulation is primarily a matter of state/territory law, reinforced by federal law in the case of AML laws or where the presence of interstate or foreign elements might otherwise frustrate the enforcement policies of state law.

FinCEN is accountable for ensuring compliance with the BSA, but does not itself directly examine FIs for compliance with that law. Instead, FinCEN has delegated examination responsibility to the IRS for state/territory licensed casino gaming
operations, other than Nevada gaming operations, as well as tribal casinos. The National Indian Gaming Commission will examine some tribal casinos pertaining to BSA casino recordkeeping and CTRC reporting requirements as part of its efforts to ensure compliance with its Minimum Internal Control Standards.

Dealers in precious metals and stones: FinCEN has delegated examination responsibility to the IRS, which examines dealers in precious metals, stones, and jewels to ensure they are complying with their obligations under the BSA. The Jeweler’s Vigilance Committee (JVC) is an industry organization that handles legal compliance for the sector. Most applicable legal requirements relate to trade practices; however, the JVC has been very proactive in educating its members about the new requirements and helping them to develop AML/CFT programs.

Other DNFBP: There are no oversight procedures for compliance with AML obligations by accountants, lawyers, real estate agents and TCSPs, since no such specific obligations have yet been introduced. However, general conduct of business oversight does exist for some of the businesses and professions, as follows.

Accountants: Accountants are subject to Codes of Professional Conduct and state licensing and accreditation. Public accountants are subject to oversight by the Public Company Accounting Oversight Board, a federal entity which was created by Sarbanes-Oxley to oversee the auditors of public companies in order to, among other things, ensure preparation of fair and impartial audit reports, strengthen auditor independence rules, increase accountability of officers and directors, and enhance the timeliness and quality of financial reports of public companies.

Lawyers: Legal professionals in the U.S. are currently subject to substantial regulation by primarily state, and to a more limited extent, federal entities, as well as self regulatory organizations, in a way that has a bearing on AML concerns.

Real estate agents: Real estate agents are governed by state law. State real estate boards (which usually have regulatory authority over real estate agents) establish licensing requirements which may include coursework and passing an examination.

Trust and company service providers: TCSPs that are not licensed with fiduciary powers under federal or state law, are not “financial institutions” under 31 USC
5312(a) (2), and are not required by law or regulation to comply with BSA requirements, such as establishing AML Programs or filing SARs. Although there is no clearly defined sector within the U.S. that provides the company formation services usually associated with TCSPs, the company laws in certain states create an environment where such services have developed significantly.
The Case

A prominent attorney operated a money laundering network which used sixteen domestic and international financial institutions, many in offshore jurisdictions.

Although the majority of his clients were law abiding citizens, a number were engaged in various types of fraud and tax evasion, and one client had committed an US$80mn insurance fraud. He charged his clients a flat fee to launder their money and to set up annuity packages to hide the laundering activity. In the event of any inquiries by regulators or law enforcement officials, the attorney were prepared to give the appearance of legitimacy to any withdrawals from the "annuities".

One of the methods of laundering used was for him to transfer funds from a client into one of his general accounts in the Caribbean. The account was linked to the attorney in name only, and he used it to commingle various client funds, before moving portions of the funds accumulated in the general account via wire transfers to accounts in other countries in the Caribbean. When a client needed funds, they could be transferred from these accounts to a U.S. account in the attorney's name or the client’s name. The attorney indicated to his clients that they could "hide" behind the attorney-client privilege if they were ever investigated.

Another method of laundering funds was through the use of credit cards. The attorney arranged for credit cards in false names to be issued to his clients. When funds were needed, the client could use the credit card to make cash withdrawals at any automated teller machine in the United States. Once a month the Caribbean bank would debit the attorneys account in order to satisfy the charges incurred by his clients. The attorney knew the holders of the credit cards.

Result

The attorney pleaded guilty to money laundering.

Lessons

Banks should follow "know your customer" procedures when issuing credit cards. In this case, the banks were issuing the credit cards to the attorney, for onward issuance to his clients.

Investigators should be aware that in a number of countries lawyer/attorney-client privilege is not applicable if the lawyer/attorney and his client are directly involved in criminal activity, and they should consult prosecutors if such an issue arises. (JMLSG, 2010)
India

The PMLA does not apply to the DNFBP sectors With the exception of casinos. There are no AML/CFT obligations for lawyers and accountants or gem and jewellery dealers. There seem to be some customer due diligence and record keeping obligations for gold dealers, as importers and authorized purchasers are registered and under supervision of the RBI (FATF, 2010).

Iran

According to article 18 of Executive By- Law, the board of directors of trades union of the designated non- financial businesses and professions shall have to introduce a unit to be responsible for anti- money laundering activities to the SCS subject to their organizational scope and expansion. They shall, proportionate to the scope of their organizations, make the necessary arrangements in a manner to obtain the assurance required for the enforcement of the law and regulations governing the anti- money laundering activities.
3.4 Legal Persons and Arrangements and Non–Profit Organizations

3.4.1 Legal Persons

U.K

According to report of FATF (2007), the UK’s approach to preventing the unlawful use of legal persons and legal arrangements for ML and FT relies on the investigative and other powers of law enforcement, regulatory, supervisory, and other competent authorities to obtain or get access to information. Such information on beneficial ownership may be available from four sources:

- ‘Open source’ data;
- Information retained by AML/CFT regulated businesses as part of their compliance obligations;
- Information held by public bodies such as the companies’ registrar or the tax authorities;
- Information held by private companies or individuals.

Powers under POCA and SOCPA for use in money laundering and related investigations into the proceeds of crime allow the financial investigator to gain access to beneficial ownership data maintained on a given company by that business, provided that beneficial ownership information is maintained there.

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Types of companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Public companies</td>
</tr>
<tr>
<td>2</td>
<td>Private Companies</td>
</tr>
<tr>
<td>3</td>
<td>Limited partnerships</td>
</tr>
<tr>
<td>4</td>
<td>Limited Liability Partnerships</td>
</tr>
<tr>
<td>5</td>
<td>Assurance companies</td>
</tr>
<tr>
<td>6</td>
<td>Industrial &amp; Provident Societies</td>
</tr>
<tr>
<td>7</td>
<td>Incorporated by Royal Charter</td>
</tr>
<tr>
<td>8</td>
<td>Special Acts of Parliament</td>
</tr>
<tr>
<td>9</td>
<td>European Public Limited Liability Companies</td>
</tr>
<tr>
<td>10</td>
<td>European Economic Interest Groupings (EEIGs)</td>
</tr>
</tbody>
</table>

Table 3.1 Types of companies in the U.K
All limited companies in the UK are registered at Companies House, an Executive Agency of the Department of Trade and Industry. The main functions of Companies House are to:

- incorporate and dissolve limited companies;
- examine and store company information delivered under the Companies Act and related legislation; and
- make this information available to the public.

**Companies Act companies**

Companies Act companies are established by registering certain documents prescribed under the Companies Act 1985 with the registrar of companies (there are separate registrars of companies for companies registered in England and Wales, Scotland and Northern Ireland). These documents include constitutional information about the company and details of those involved in its formation (notably its first directors and members). On registration, companies are given a “certificate of incorporation” and a unique identifying number. Companies Acts companies are owned and, ultimately, controlled by their members. A company’s members are those persons whose names are entered on its register of members. All Companies Act companies are required to have a registered office in the UK. Companies are required to keep an up to date register of the names and addresses of its members, which is to be kept available for inspection by the public.

**Non-Companies Act companies**

Non-Companies Act companies are required to notify the registrar of their principal office in the UK. Although such companies are not subject to registration on incorporation in the same way as Companies Act companies, they are subject to much the same regime of ongoing disclosure as regards as Companies Act companies.
Partnerships

Partnerships are owned and controlled by the partners. Limited partnerships and limited liability partnerships (LLPs) must disclose to the registrar information about their names, the general nature of their business, their principal place of business, the partners’ names, the term (if any) for which the partnership is entered into, and the sums contributed by the limited partners.

UK-specific forms of body corporate

Friendly Societies, Industrial Provident Societies, Co-operative societies and Building Societies have a range of applicable legislation under which they can become incorporated. All are entered onto registers maintained by the FSA. Basic registration documentation matching that required for companies is required. In addition, building societies are directly regulated by the FSA as part of its mainstream financial regulation role.

U.S.

According to the report of FATF (2007), in preventing the use of legal person for illicit purposes, the U.S. government primarily relies on an investigatory approach. The U.S. uses a combination of the following mechanisms:

- corporate reporting requirements.
- general purpose compulsory powers available to certain law enforcement, regulatory supervisors and judicial authorities during an investigation; and
- a tax registration system for employers administered through the issue of Employer Identification Numbers (EIN)

The Department of Justice and other federal law enforcement entities (including DEA, FBI, and ICE), in addition to the Internal Revenue Service(IRS), Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) have general purpose compulsory powers enabling them to obtain beneficial ownership and control information for legal persons created in, or operating in, the U.S. These powers are triggered when illicit activity is suspected.
Table 3.2 Types of companies in the U.S

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Types of companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Public companies</td>
</tr>
<tr>
<td>2</td>
<td>Private Companies</td>
</tr>
<tr>
<td>3</td>
<td>Federally incorporated</td>
</tr>
<tr>
<td>4</td>
<td>N.A. (National Association), a designation used by national banks</td>
</tr>
<tr>
<td>5</td>
<td>NT&amp;SA (National Trust and Savings Association), a less common designation used by national banks</td>
</tr>
<tr>
<td>6</td>
<td>Federal Credit Union</td>
</tr>
<tr>
<td>7</td>
<td>Federal Savings Bank</td>
</tr>
<tr>
<td>8</td>
<td>State incorporated</td>
</tr>
<tr>
<td>9</td>
<td>Corp., Inc. (Corporation, Incorporated)</td>
</tr>
<tr>
<td>10</td>
<td>General partnership</td>
</tr>
<tr>
<td>11</td>
<td>LLC, LC, Ltd. Co. (limited liability company)</td>
</tr>
<tr>
<td>12</td>
<td>LLLP (limited liability limited partnership)</td>
</tr>
<tr>
<td>13</td>
<td>LLP (limited liability partnership)</td>
</tr>
<tr>
<td>14</td>
<td>LP (limited partnership)</td>
</tr>
<tr>
<td>15</td>
<td>Professional corporations</td>
</tr>
<tr>
<td>16</td>
<td>Sole proprietorship</td>
</tr>
</tbody>
</table>

In the United States, the individual states incorporate most businesses, and some special types are incorporated by the federal government. Corporate law is primarily handled at the state level. Many states follow the Model Business Corporation Act that was developed in 1984 to encourage uniformity amongst the state corporation laws. Many states have supplemented their general corporation statutes with special statutes providing relaxed rules for closely held corporations that elect to take advantage of their provisions or allow for the creation of hybrid or special purpose entities such as business trusts.

The U.S. relies on a combination of systems and measures to satisfy the requirements for access by authorities to accurate and current information on the beneficial ownership and control of legal persons upon suspicion in order to investigate money laundering. At both the federal and state level there is a range of investigatory powers available to law enforcement and certain regulators to compel the disclosure of ownership information (FATF, 2007).
India

In India companies are created, registered and regulated under the Companies Act 1956. India has a central registry, the Registrar of Companies Affairs (RCA), for legal Persons. All persons wishing to form a company must register with the RCA.

In India Companies fall into three categories: private companies, unlisted public companies and listed public companies. For private companies, subscribers must inform the RCA of any additional shareholders and describe the make up of and changes to the board, as well as at each year’s end, the changes to or relinquishing of ownership of shares. For unlisted public companies, the RCA performs the technical scrutiny of the final accounts, and full disclosure requirements are necessary, similar to that of private companies. For publicly listed companies, shares are not held in physical form, and any changes to the make up of ownership must be submitted to the registrar yearly accompanied by formal third party audit. The RCA does not intervene in a publicly listed company's affairs unless a shareholder specifically communicates to the RCA – at which time they can recommend for investigation to the Serious Frauds Investigation Office.

Iran

Iran has different well structured laws and regulations applicable to both domestic and foreign companies working in Iran such as commercial code company law, import and export regulations, labor law, social security regulations, taxations, industrial and intellectual property protection, foreign national entry. Resident and work permits, Banking and insurance etc.

According to the Iranian Commercial Code, there are 7 types of companies all of which must be duly established and registered in order to have legal personality. Although this system was not set up to prevent ML from entering into legal businesses as such, it is considered to be a possible tool for that purpose. It is possible to discourage (organized) criminals from registering their business if registration officers pay specific attention to this issue and if co-operation and information exchange with other agencies and law enforcement is established (Council of Europe, 2003). All types of companies under Iranian law are:
1. Joint Stock Company

- Public Joint Stock Company whose promoters secure a portion of its share capital by way of transferring shares to the public and such a company is called a public company.

- Private Joint Stock Company whose share capital, in its entirety, is secured by its promoters at the time of its formation and such a company is called a private company.

2. Limited Liability Company

3. General Partnership Company

4. Limited Partnership

5. Joint Stock Partnership

6. Proportional Liability Partnership

7. Cooperative Company

- A Producers Cooperative Company is one formed between producers and artisans for the production and sale of goods that they produce in common.

- A Consumers Cooperative Company is one formed for the following purposes:
  
  (i) Sale of Articles necessary to life either produced by the members or purchased by them.

  (ii) Distribution of profits and losses between members in proportion to the purchases made by each of them.

3.4.2 Legal Arrangements

Legal Arrangements express trusts or other similar legal arrangements. A trust is a relationship whereby property (including real, tangible and intangible) is managed by one person (or persons, or organizations) for the benefit of another. A trust is created
by a settler (or feoffor to uses), who entrusts some or all of their property to people of their choice (the trustees or feoffee to uses).

Trusts which attract legitimate asset protectors also attract money launderers. Many of the techniques of asset protection, particularly layering, are techniques of money-laundering also, and innocent trustees such as bank trust companies can become involved in money-laundering in the belief that they are furthering a legitimate asset protection exercise, often without raising suspicion.

**U.K**

Trusts are a long-standing, popular, and integral part of the legal and economic landscape of the UK. A trust does not count as a legal person or a contract, nor can it own property. However, trusts allow individuals to dispose of their assets according to their particular objectives and for a range of other legitimate and economically important activities.

A trustee must maintain accurate records of the trust property. They must allow a beneficiary, or his solicitor to inspect those accounts and the trustee must be prepared to give full information as to the value of the trust fund. If trust money is invested, the trustee must on request, supply a beneficiary with details of those investments. These obligations largely stem from the common law, although the investment activities of trustees are covered by different pieces of statute law in England & Wales, Northern Ireland, and Scotland. The UK’s approach to preventing the unlawful use of legal arrangements for ML and FT relies on the investigative and other powers of law enforcement, regulatory, supervisory, and other competent authorities to obtain or get access to beneficial ownership information. Such information is available from three sources:

- Information retained by AML/CFT regulated businesses as part of their compliance obligations;
- Information held by public bodies such as the tax authorities or charity regulators;
- Information held by private companies or individuals.
U.S

In the U.S. a trust is a legal entity that is created under state law. The IRS retains oversight of income generated by trusts through federal tax laws. Trusts are subject to the same general investigative powers exercised by those regulators and law enforcement agencies, beneficiaries have some corporate reporting requirements under the Securities Exchange Act, and trusts also have obligations to apply for an EIN. The income of a trust is required to be reported via IRS Form. These returns are required to include the name and taxpayer identification number of each beneficiary deemed to have received a distribution from the trust for that year, as well as the amount to be reported as income by that beneficiary.

According to FATF (2006) the U.S. relies on a combination of systems and measures to satisfy the requirements for access by authorities to accurate and current information on the beneficial ownership and control of trusts. This includes the investigatory powers available in respect of legal persons. Under U.S. law, the IRS has access to beneficial owner information when distributions are made to the beneficiary or income is earned by the trust.

India

The PMLA does not apply to the DNFBP sectors With the exception of casinos. There seem to be some customer due diligence and record keeping obligations for gold dealers, as importers and authorized purchasers are registered and under supervision of the RBI (FATF, 2010). Under the RBI's AML guidelines, banks are required to verify the identity of trustees, settlers, grantors, protectors, beneficiaries and signatories. Records of these parties are required to be maintained in line with standard record-keeping procedures, and will be available to the authorities in the course of inspections or on demand.

Iran

In Iran foundations and charities are under anti-money laundering regulation. According to Article 20 of Executive By-Law Organization of Endowment and Charity Affairs shall in their normal inspection tours, have to take account of the rules for combating money laundering and terrorist financing and comment on the
compliance or non-compliance with such rules. The SCS shall have to examine the performance of Organization of Endowment and Charity Affairs once every six months and report the matter to the Anti-Money Laundering supreme Council.

3.4.3 Non-profit Organizations

A non-profit organization (NPO) is an organization that does not distribute its surplus funds to owners or shareholders, but instead uses them to help pursue its goals. Examples of NPOs include charities, trade unions and public arts organizations. Most governments and government agencies meet this definition, but in most countries they are considered a separate type of organization and not counted as NPOs. They are in most countries exempt from income and property taxation.

U.K

Regulation and supervision of the charity sector is undertaken by the Charity Commission of England and Wales (“the Charity Commission”) in England and Wales and the Office of the Scottish Charities Regulator (“the OSCR”) in Scotland. Charities in England & Wales are required to formulate accurate accounts, with disclosure levels appropriate to their level of income and expenditure, and keep these accounting records for a period of 6 years. Charities in England and Wales are required by statute to submit financial information to the Charity Commission on an annual basis.

U.S

According to U.S. law, any person or group may establish a charitable organization, and the creators of the organization are free to choose any charitable endeavour they wish to pursue. After a recognized type of legal entity has been formed at the state level, it is customary for the nonprofit organization to seek tax exempt status with respect to its income tax obligations. That is typically done by applying to the Internal Revenue Service (IRS), although statutory exemptions exist for limited types of nonprofit organizations. The NPO sector is monitored by the federal government and state authorities. Transparency is facilitated by federal tax laws, which provide that
most information reported by tax-exempt NPOs to the Tax Exempt and Government Entities Division (TEGC) of the IRS is available to the public.

The other main transparency mechanisms include the certification program for USAID. Charities operating in the U.S. are also subject to self-regulation managed by umbrella and watchdog organizations. The U.S. states and the District of Columbia oversee the fund-raising practices of charities domiciled or operating in their jurisdictions. Many of the larger states have a separate agency to oversee charities, including the Offices of the Attorneys General and State Charities Officials. Thirty-nine U.S. states require any charity to register before soliciting funds within the state, no matter where the charity is domiciled.

The measures which are being implemented to ensure that the NPO sector cannot be abused by terrorists or terrorist financiers are working effectively. U.S. authorities at both a state and federal level take action against illegitimate or fraudulent charities particularly where they are able to demonstrate that these charities have been established to facilitate terrorist financing.

India

In India, NPOs are commonly known as Non-Governmental Organizations (NGOs). They can be registered in four ways:

- Trust
- Society
- Section-25 Company
- Special Licensing

Registration can be done with the Registrar of Companies (RoC). The following laws or Constitutional Articles of the Republic of India are relevant to the NGOs:

- Articles 19(1)(c) and 30 of the Constitution of India
- Income Tax Act, 1961
- Public Trusts Acts of various states
Non-profit organizations can be registered either as an unlimited company under Section 25 of the Companies Act or a Society under the Societies Registration Act. Some charities function as Trusts, in which case the Trust Deed is registered with the Registrar of Properties. They are also required to have an office. Information as to subscribers and accounts is to be furnished to the Registrar of Societies, which is public information. Societies are also required to maintain a Register of Members. Mutual Funds are also registered as Trusts but they need to be managed by an asset management company which must be registered under the Companies Act.

Persons with common economic interest may constitute themselves into a cooperative society. Cooperatives are regulated under the States’ Cooperative Societies Acts. Cooperatives having businesses in more than one State may be governed by the Multi-State Cooperative Societies Act, of the Union.

**Iran**

In Iran, NPOs are known as Non-Governmental Organizations (NGOs). The NGOs fall under the general definition of non-commercial organizations. Current laws within the Iran have enabled NGOs to form and pursue a variety of non-profit and non-political objectives. NGOs can be formed by either natural persons or legal entities. All NGOs, after obtaining the necessary permit from the appropriate supervisory board, must register with the Registration Office of Companies and Industrial Units, Bureau of Non-Commercial Organizations. This bureau is a department of the Ministry of Justice and maintains the NGO registry, which provides the name, purpose, founders, and addresses of all registered NGOs. The NGOs sector is monitored by the government.
3.5 National and International Co-operation

The international community has recognized that the problems of money laundering and terrorism require a coordinated approach. No individual country has the power to stop money laundering – if one country is hostile to laundering, criminals simply look elsewhere for a place to clean their money. National and International cooperation is therefore essential and it is thus important to seek increased global awareness and cooperation to curb the success of money laundering. Hence, adopting, implementing, and enforcing internationally accepted standards against money laundering and the financing of terrorism are on the agenda of countries.

3.5.1 National Co-operation and Coordination

U.K

In U.K, policy formulation on AML measures is developed through engagement with all interested parties in the Money Laundering Advisory Committee” (MLAC). MLAC is a forum for central government, law enforcement, supervisors, and the private sector that is jointly chaired by Home Office/HMT and meets periodically throughout the year to discuss how the regime is functioning and to inform advice to Ministers. Some of the Interagency working groups and task forces focused on AML/FT are as following:

The Terrorist Finance Action Group (TFAG) is a cross-Whitehall committee that forms part of the wider Whitehall framework on counter-terrorism.

The Asset Freezing Working Group (AFWG) is chaired by HMT and agrees the handling of individual asset freezing cases as well as the architecture of the UK’s asset freezing regime.

Financial Investigators Working Group (FIWG). At the FIWG, UK financial investigators regularly meet at both national and regional level (Financial Investigators Working Group - FIWG) to discuss best practice in techniques and trends.
The Concerted Inter-agency Criminal Finances Action group (CICFA) has been operational for five years. It brings together central government, regulators, and the agencies responsible for tackling acquisitive financial crime.

The Organised Crime Task Force (OCTF) in Northern Ireland, chaired by the Security Minister, provides a framework to bring together all the key agencies involved in the fight against organised crime.

The Financial Crime Information Network is a forum for intelligence-sharing on financial crime issues including money laundering and terrorist financing.

Moreover, The UK FIU has deployed mechanisms to ensure co-operation between domestic law enforcement, the reporting sectors, and other branches of SOCA. The UK FIU has a Dialogue Team whose core function is to liaise between the sectors outlined above through formal meetings, informal contact, and workshops, and to facilitate feedback and share best practice with the reporting sector in sector specific seminars. The UK FIU also has a dedicated International Team whose core responsibility is to liaise with international partners through Egmont, FIU Net, FATF, and the FSRBs.

The FSA has a statutory obligation to co-operate and co-ordinate domestically with other competent authorities to prevent and detect financial crime. The FSA has seconded personnel to the UK FIU and UK FIU terrorist finance team to enhance co-operation between the organizations. The FSA has also agreed a number of MOUs with other UK authorities such as the Association of Chartered Certified Accountants, the Association of Chief Police Officers, HMRC, and Institute of Actuaries.

HMRC has two research and analysis divisions: The Centre for Exchange of Intelligence (CEI) and the Centre for Research and Intelligence (CRI). Both make frequent disclosures to UK law enforcement agencies. Moreover, HMRC’s FNIU and SOCA work closely together on money laundering projects where both parties have a common interest.

It can be concluded that, the UK has a comprehensive system for domestic cooperation to combat ML/FT, at both the policy and the operational levels. Internal cooperation and coordination between UK policy makers, the FIU, law enforcement
and supervisors and other competent authorities is effective. There also appears to be effective co-operation amongst agencies on an operational level.

U.S.

National policy to combat money laundering is primarily coordinated by the Treasury in the context of the Money Laundering Working Group. The Money Laundering Working Group focuses on a wide range of AML/CFT issues and cooperates on specific courses of action relative to particular issues or concerns. Chaired by the Treasury Department/TFFC, it includes representative from the DOJ, State Department, DHS, FinCEN, law enforcement agencies and financial regulators.

The U.S. authorities also consult with the Bank Secrecy Act Advisory Group (BSAAG) which is comprised of representatives from the Treasury, FinCEN, the DOJ, the Office of National Drug Control Policy, various law enforcement agencies, financial regulatory agencies (including SROs and state regulatory agencies) as well as financial services industry representatives which are subject to BSA regulation.

Some of Interagency working groups and task forces focused on AML are as following:

- High Intensity Financial Crime Areas (HIFCAs): HIFCA Task Forces seek to improve the quality of federal money laundering and other financial crime investigations by concentrating the expertise of the participating federal, state and local agencies in a unified task force that can utilize all of the FinCEN, DEA/SOD and DHS/ICE MLCC financial databases.

- Organized Crime Drug Enforcement Task Forces (OCDETF): Led by the DOJ, the following agencies also participate in the OCDETFs: the DEA, FBI, the Department of Alcohol Tobacco and Firearms, the USMS, the IRS, ICE and the U.S. Coast Guard—in cooperation with the DOJ’s Criminal and Tax Divisions, the 94 U.S. Attorneys’ Offices (USAOs), and state and local law enforcement.

- Drug Enforcement Administration Special Operations Division (DEA/SOD): DEA is a law enforcement agency under the united state Department of

195
Justice, tasked with combating drug smuggling and use within the United States. The DEA/SOD is a DEA-led division with participation from ICE, CBP, the FBI, the IRS and DOJ’s Criminal Division.

Money Services Business Working Group (MSB-WG): The MSB-WG is comprised of representatives from ICE, IRS, FinCEN, Treasury, the FBI the DEA and members of the intelligence community.

Moreover, there is a significant amount of coordination and cooperation amongst regulatory agencies in the banking sectors, most of which is formalized through a series of MOUs. In the securities sector, FinCEN is in the process of finalizing memorandum of understandings (MOUs) with the SEC and the CFTC. In the insurance sector, coordination among the various state/territorial supervisors/regulators is facilitated through the NAIC. This is a voluntary organization of chief insurance regulatory officials from 50 U.S. states, the District of Columbia and four U.S. territories. In the MSB sector, interagency coordination is formalized by MOUs. The IRS has signed MOUs with FinCEN and with individual states to share examination information and leverage examination resources at the state and federal levels. Coordination amongst state MSB regulators is facilitated by the Monster Truck Racing Association (MTRA). The MTRA is a national non-profit organization that works towards the effective and efficient regulation of money transmitters and check sellers.

India

The Economic Intelligence Council (EIC) has been established to enhance coordination between various enforcement agencies and departments in the Ministry of Finance. The EIC provides a forum for enforcement agencies to exchange intelligence, to formulate common strategies to combat economic offences, to strengthen operational coordination and to discuss cases requiring inter-agency coordination. Members of the EIC are from different government agencies, including Company Affairs, the RBI, the SEBI, Income Tax, the Director General of Revenue Intelligence, Customs and Central Excise, the NCB, the CBI, and the Intelligence Bureau. There are 18 Regional Economic Intelligence Committees (REIC) in India which function similarly as the EIC at the regional level. Meetings of the EIC and
REIC are conducted monthly to enable all member agencies to update each other on recent developments relating to economic crimes.

The Central Economic Intelligence Bureau (CEIB) was been set up in 1985 as the SCS for the Economic Intelligence Council. The CEIB was set up to coordinate the intelligence gathering and enforcement activities of economic intelligence in the area of economic offences.

**Iran**

In order to make coordination among the appropriate authorities/establishments aimed at collecting, processing and analyzing the news, records, documents, information and reports submitted; operating the intelligent (smart) database systems; identifying the suspicious transactions and for the purpose of combating the money laundering offence or offences, the Anti-Money Laundering supreme Council was set up under the chairmanship and whit the responsibility of the Minister of Economic Affairs and Finance and whit membership of the Governor of the Commerce, Minister of Intelligence, Minister of Interior and the Governor of the Central Bank. One of the functions of SCS is to provide coordination among the appropriate authorities and establishments and pursue the full enforcement of law across the country. The SCS shall be based in the Minister of Economic Affairs and finance (Article 4 of AML law).

**3.5.2 The Conventions**

A convention is a set of agreed, stipulated or generally accepted standards, norms, social norms or criteria, often taking the form of a custom. Certain types of rules or customs may become law and regulatory legislation may be introduced to formalize or enforce the convention.

The term convention is also used in international law to refer to certain formal statements of principle such as the Vienna Convention. Conventions are adopted by international bodies such as the U.N. Conventions so adopted usually apply only to countries that ratify them, and do not automatically apply to member states of such
bodies. These conventions are generally seen as having the force of international treaties for the ratifying countries.

U.K


U.S


India

India is a party to the 1988 UN Drug Convention, and is a member of the Asia/Pacific Group (APG) on Money Laundering. India implements the 1988 UN Drug Convention through amendments to the NDPSA (in 1989 and 2001) and the PMLA. It is a signatory to, but has not yet ratified, the UN Convention against Transnational Organized Crime. India signed the United Nations Terrorist Financing Convention on 8 September 2000 and ratified it on 22nd April, 2003. India is a party to the UN International Convention for the Suppression of the Financing of Terrorism. India acceded to the Vienna Convention on 27th March, 1990 and signed the Palermo Convention on 12th December, 2002. India is not a party to the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.
Iran

Iran is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Iran has signed but not ratified the UN Convention against Corruption. It has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

Iran is not a party to the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

3.5.3 Mutual Legal Assistance

A mutual legal assistance is an agreement between two countries for the purpose of gathering and exchanging information in an effort to enforce public laws or criminal laws. This assistance may take the form of examining and identifying people, places and things, custodial transfers, and providing assistance with the immobilization of the instruments of criminal activity.

U.K

According to the Criminal Justice (International Co-operation) Act 1990 the UK is able to provide a full range of legal assistance in criminal matters. Assistance for investigations, prosecutions and related proceedings is provided either through the UK’s central authorities or through the UK National Central Bureau of Interpol. In particular circumstances the HMRC can act as a central authority for MLA on fiscal matters relating to England, Wales, and Northern Ireland, and the Northern Ireland Office can handle certain cases related solely to Northern Ireland where the treaties or conventions allow it.

U.S

The Office of International Affairs of the Department of Justice (OIA), as the conduit for mutual legal assistance (MLA) requests coordinates all international evidence gathering. OIA has attorneys and support staff with responsibilities and expertise in various parts of the world and different substantive areas. OIA and other U.S. authorities helping OIA to execute foreign requests have the authority to obtain
documents and information for use in ML and FT investigations and in prosecutions and related proceedings. FinCEN also has the authority to respond to requests for lead information and has procedures in place to facilitate this. FATF (2006) reported that the U.S. MLA system is generally comprehensive and robust.

**India**

The general power to provide mutual legal assistance in criminal matters is through the Code of Criminal Procedure 1973; however India can provide MLA for specific matters through a number of other Acts such as the NDPS Act and the Customs Act. Chapter IX of the PMLA contains separate MLA provisions specifically for assistance in money laundering cases. The MLA provisions in the PMLA will allow for a broad range of assistance to be provided in money laundering cases. Most of the search and seizure powers available under the Act for domestic offences in sections 17 and 18 will be available for MLA requests. For example, production, search, seizure of documents and taking witness statements are available through sections 59(2) (d) (ii) and 59(2) (c), service of documents is available through section 59(2), sections 60(3) and 60(6) allow for tracing and ID of property and for attachment and confiscation of property in accordance with the Act. Sharma (1998) stated that, India has made mutual legal assistance arrangement with several countries. Some of concluded agreements on mutual legal assistance are India and U.K (1992), India and Russia (1993), India and China (1996).

**Iran**

According to Article 12 of AML law, in the circumstances where the law of the Legal and Informational Assistance in Combating the Money Laundering activities has been approved between the Government of the Islamic Republic of Iran and other countries, the inther-collaboration shall take place in conformity with the conditions set forth in the agreement.

There is an agreement between Iran and India on mutual legal assistance in criminal matters. It will provide a broad legal framework for bilateral cooperation with the India in the investigation and prosecution of crime, tracing, restraining or forfeiting of the proceeds and instruments of crime.
3.5.4. Extradition

Extradition is the official process whereby one nation or state surrenders a suspected or convicted criminal. Between nation states, extradition is regulated by treaties. Where extradition is compelled by laws, such as among sub-national jurisdictions, the concept may be known more generally as rendition. Extradition is possible pursuant to multilateral conventions, such as Article 3 of the Vienna Convention (for narcotics-related money laundering offenses) and Article 6 of the Palermo Convention (for organized crime offenses).

**U.K**

The Extradition Act 2003 which allows for extradition came into force on 1<sup>st</sup> January, 2004. Money laundering and terrorist financing are extraditable offences in the UK. The UK can also extradite its own nationals.

**U.S**

According to U.S law, money laundering is an extraditable offense for requests made under the dual criminality treaties. The United States extradites defendants only if there is a bilateral extradition treaty between the U.S. and the requesting state. The U.S has no law barring the extradition of its nationals. Moreover, the Secretary of State may authorize the extradition of U.S. nationals even in cases where the applicable bilateral extradition treaty does not require the extradition of nationals.

**India**

India signed the United Nations Terrorist Financing Convention on 8<sup>th</sup> September, 2000 and ratified it on 22<sup>nd</sup> April, 2003. India has largely implemented the Terrorist Financing Convention through the Unlawful Activities (Prevention) Act (UAPA). This Convention is also implemented through the Code of Criminal Procedure 1973 and the Extradition Act 1962. Terrorist financing is an extraditable offence under Indian law pursuant to the Extradition Act 1962. Extradition under the PMLA will only be possible if the money laundering offence relates to one of the predicate offences listed in the Schedule to the PMLA.
Iran

According to Article 12 of AML law, in the circumstances where the law of the Legal and Informational Assistance in Combating the Money Laundering activities has been approved between the Government of the Islamic Republic of Iran and other countries, the inther-collaboration shall take place in conformity with the conditions set forth in the agreement. Iran has an extradition treaty with India. This treaty provides a legal framework for seeking extradition of terrorists, economic offenders, and other criminals from and to India.

3.6 Consequences of Laws on AML

Though academically it could be discussed that ML may prove useful in certain context, in light of the harmful effects of ML posed above no one would argue against the AML laws. There are various motivations to have an AML mechanism in place. To begin with, at the most basic, the rationale is to support the adage that “crimes don’t pay”. Firstly, there is the moral dimension: crime should not pay. It is simply not acceptable to society that a person who does wrong should benefit as a result. Apart from the aforesaid dimension, it is intended to deprive the criminal organization of their “financial lifeblood.” Moreover, if it is shown that crime does not pay would act as a sufficient deterrent, as few theorists suggest for cost- benefit analysis, especially in economic crimes like ML. Further, there is another theory that if criminals can be prevented from profiting from their offences, they will not be able to re-invest money in those various ways and hence will be hampered from committing further offences. Equally, if the victims of crime, or even just the law abiding public, see criminals enjoying a very comfortable life, far more comfortable than their own, this will lead to a considerable public disquiet. Further, we live in a globalized world as a community and have international relations at stake. There are pressures from parent organizations to which one has acceded to as well as pressures from the developed countries for compliance to tough AML regimes. The compliance results in better international status of the country.

AML law is necessary because money laundering tends to corrupt even the most professional players in the market. Now a money launderer can be a white collar
businessman doing the business legitimately. However, when lured by low interest rate loans (given from proceeds of crime), he would be tempted to launder the black money for that purpose. This illegal business in the long run contaminates the legal business and profession, for example, ML needs lawyers and the lure of money can transform the noble professionals to criminals (which they do not perceive they are doing). ML promotes corruption and bribery in every sector, specifically the banking sector. Bribe is just like human blood to the tongue of a wild cat, which once gets the taste of it, cannot resist killing humans. Thus ML is an activity which is capable of corrupting a chain of financial institution. This provides a sufficient rationale for having an AML law which acts like a slow poison, though to some it may seem as power vitamin.

The activities of powerful criminal organizations can have catastrophic economical, social and even political consequences. Laundered money provides drug traffickers, arms dealers and other criminals with the wherewithal for operating and developing their enterprises. Unless remedies are found, ML can strike at the integrity of a country's financial institutions. The very fact of billions of dollars are being removed each year from normal economic activities constitutes a real threat at a time when the financial health of every country affects the stability of the global marketplace. ML erodes the credibility and, hence, stability of financial markets: if a bank collapses as a result of organized crime, the entire financial system of the country or even the whole region can suffer through the contagion effect.

Therefore, laws and regulations are key tools in the fight against this phenomenon. The passage of a law has more consequences, including economical, political - social and legal. Enacting Anti-money laundering laws in order to eliminate ML is considered a major step. Under these laws, combating money laundering will find the legal status and government and people are required to have a coherent and unified action in relation to ML. A comprehensive and effective law significantly reduces the profitable aspects of criminal activity and discourages criminals from utilizing a country. An effective law for AML has important consequences, for a country. These consequences include lower levels of ML crime, increased stability of financial institutions, positive effects on economic growth and enhanced risk management techniques for the country’s FIs. Sections 3-1 to 3-4, in this chapter provides a
summary of the AML laws in place in the U.K, U.S, India and Iran. Main consequences of these laws on AML are as following:

### 3.6.1 Main consequences of laws on AML

#### Fighting Crime

Undoubtedly, a strong AML law that includes criminalization of ML and a broad scope of predicate offenses for ML helps to fight crime. In this regard, confiscation and forfeiture of money laundering proceeds are crucial to the success of any AML program. Forfeiture of money laundering proceeds eliminates those profits altogether, thereby reducing the incentive to commit criminal acts. Thus, it should go without saying that the broader the scope of predicate offenses for money laundering, the greater the potential benefit. As mentioned above, one of the important consequences of law in the fight against ML is criminalization of it. The AML laws, in about developed and DGCs criminalized money laundering. These laws, particularly in DDCs, provide a list of predicate offences which covers to a large extent each of the 20 designated categories of offences. Liability for money laundering applied to both natural and legal persons. All of offences under the AML laws are punishable. Also, except of Iran, terrorist financing is criminalized under laws in the U.K, U.S and India. Terrorist financing is a predicate offence for money laundering.

#### Stability of Financial Institutions

Customer identification and due diligence procedures, also known as “know your customer” rules, are part of AML law. These rules are not only consistent with, but also enhance, the safe and sound operation of FIs. These policies and procedures are an effective risk management tool.

#### The public confidence

To the public confidence, an effective AML law reduces the potential that the institution could experience losses from crime. AML laws in DDCs provided a proper customer identification procedures and determination of beneficial ownership provide specific due diligence for higher risk accounts and permit monitoring for suspicious
activities. Such prudential internal controls are consistent with the safe and sound operation of a financial institution.

**Encouraging Economical growth**

As previously stated, ML has a negative effect on the economic growth of countries. Because, money launderers tend transform productive enterprises into sterile investments by operating them for the primary purpose of laundering illegal proceeds, rather than as profit-generating enterprises. AML law in DDCs provides a disincentive for the criminal involvement in the economy. This permits investments to be put into productive purposes that respond to consumer needs and help the productivity of the overall economy.

**Establishment of FIU**

For combating against ML, establishing a central agency responsible for receiving, requesting and analyzing is vital. Establishment of financial intelligence units is one of the consequences of law on AML. In accordance with the law, U.K, U.S. India and Iran established and designated a central agency responsible for receiving, requesting, analyzing and disseminating to the competent authorities, disclosures of information relating to financial transactions that are required to be reported pursuant to their regulations that concern suspected proceeds of crime.

**Appointment of Money Laundering Authority (MLA)**

Appointment of a person or persons to be known as the MLA to supervise FIs is one of consequences of laws in DDCs and DGCs. Laws give the power and responsibility to the MLA. The MLA is responsible to receive the reports issued by financial institutions, send any such report to the law enforcement authorities, destroy any note or copy thereof made or taken pursuant to the provisions and create training requirements and provide such training for any FI in respect of the business transaction record keeping and reporting obligations.

**Freezing of Property**

Laws, in both DDCs and DGCs, allowed the court or other competent authority may order, in accordance with the law, the freezing, seizure, or forfeiture of any property,
proceeds or instrumentalities. Competent authority upon application to a judge of the (Supreme) Court and satisfying him that the authority has charged or is about to charge a person with a ML offence may apply for an order freezing the property of or in the possession or under the control of that person wherever it may be.

Creating the responsibility for FIs

FIs are highly likely to be abused by launderers as channels through which they put their money into the legitimate financial system. Hence, one of more important consequence of law is creating the responsibility for FIs in relation to the fight against ML.

AML laws in the U.K, U.S., India and Iran engaged the FIs to maintain accounts in the name of the account holder. They do not allow opening or keep anonymous accounts or accounts which are in fictitious or incorrect names. Also, FIs shall record and verify by reliable means, the identity, representative capacity, domicile, legal capacity, occupation or business purpose of persons, as well as other identifying information on those persons, whether they be occasional or usual clients, through the use of documents such as identity documents, passports, birth certificates, driver's license, partnership contracts and incorporation papers, in addition to documents providing convincing evidence of their legal existence and the powers of their legal representatives, or any other official or private documents, when initiating or conducting business relations, especially when opening new accounts or passbooks, entering into fiduciary transactions, or performing cash transactions over an amount specified by the competent authority.

FIs in the U.K, U.S and Iran, are responsible for maintaining and keep current information during the period in which business relations are in effect, and for at least five years after their conclusion. In this regard, FIs in India must maintain and keep current information for at least ten years. Also, in accordance with the law, FIs in DDCs and DGCs, shall comply promptly, and within the period of time to be established, with information requests from the competent authorities concerning the records of information and documentation, for use in criminal, civil, or administrative investigations, prosecutions, or proceedings, as the case may be, regarding illicit traffic or other serious offenses. FIs do not allow notify any person, other than a court
or other person authorized by law, that information has been requested by or furnished to a court or other competent authority. Undoubtedly, identification and verification of customers and record keeping could play a key role in fight against ML and FT.

**Money Laundering an Offence for Extradition Purposes**

Another legal consequence of law on AML is the purposes of any law relating to extradition or the rendition of fugitive offenders, ML is an offence for which extradition or rendition may be granted.

**Mutual assistance in relation to Money Laundering**

This obligation reflects the provisions of the Vienna Convention against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances and also international mutual assistance practice. AML laws in the U.K and U.S allow a competent authority to obtain a warrant to search premises for information or evidence required by a foreign State which is investigating or prosecuting a money laundering case.

**3.6.2 Public awareness and AML Laws**

Experience abroad has shown that, in the early stages of implementation, it is important for the Government to take a proactive role in promoting the Act and making the public aware of the law and how they can use it. Increasing the public awareness could have a positive impact on successes of Laws and regulations. Therefore, countries should develop and organize public awareness programmes.

Public awareness has an important function within the FIs. It provides the template for shaping client’s behavior, perception and understanding of events such as ML. Public awareness activities foster changes in behavior leading towards a culture of risk reduction. This involves public information, dissemination, education, radio or television broadcasts, use of printed media, as well as the establishment of information centers’ and networks and community and participation actions (Sharma, 1998), (Singh, 2007).
To raise public awareness of the magnitude of the threat posed by ML and TF to the economy and public safety, the countries should be launch a public awareness and education programmes. In DDCs the AML model the public sector, is not alone in its efforts to control ML. In order to comply with the DDCs laws effectively, the private sector must constantly communicate with the government. But, the DGCs the private sector has not yet been fully integrated with the public sector. In this regard, U.K has a very good experience. For instance, one of more important regulatory objectives of the Financial Services Authority (FSA) - as UK’s single financial services regulator - is public awareness (Raphael, 2006).

Community Literacy rate could be a reasonably good indicator of public awareness in a community. Table 3.3 indicates that, the Literacy rate in DGCs is lower than in DDCs, whereas, relationship between consequences of AML laws with public awareness, promotion of education is a key obligation of governments in DGCs.

Table 3.3 Literacy rate in DDCs and DGCs

<table>
<thead>
<tr>
<th>Country</th>
<th>DDCs</th>
<th>DGCs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>U.K</td>
<td>U.S</td>
</tr>
<tr>
<td>Literacy Rate %</td>
<td>99%</td>
<td>99%</td>
</tr>
</tbody>
</table>

Unawareness about the problem of ML among the common people is an impediment in having proper AML regime. People in India, especially among the poor and illiterate, do not trust banks and prefer to avoid the lengthy paperwork required to complete a money transfer through a financial institution. The hawala system provides them same remittance service as a bank with little or no documentation and at lower rates and provides anonymity and security. This is because many don’t treat this to be a crime and are not aware about the harmful effects of the crime (Kumar S., 2009).

Therefore, to create client awareness, the FIs should publish the AML rules, regulations and notifications which are issued by the Government. Undoubtedly,
client awareness from AML laws and regulations has a positive impact on combating ML.

3.6.3 Legal punishment and AML Laws

Punishment is the authoritative imposition of something negative or unpleasant on a person in response to behavior deemed wrong by an individual or group. The authority may be either a group or a single person, and punishment may be carried out formally under a system of law or informally in other kinds of social settings. The object of punishment is to reform the offender; to deter him and others from committing like offences; and to protect society.

Legal punishment involves some pain or penalty that is warranted by law, inflicted on a person, for the commission of a crime or misdemeanor, or for the omission of the performance of an act required by law, by the judgment and command of some lawful court.

According to international Conventions and standards such as; The UN Convention against illicit traffic in Narcotic Drugs and Psychotropic substances (1988), countries are under an obligation to criminalize money laundering in their domestic legal systems and to set penalties for those who commit such as these crimes in accordance with international norms and also with their domestic legislations.

Pursuant to FATE Recommendation 17, Countries should ensure that effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, are available to deal with natural or legal persons covered by these Recommendations that fail to comply with anti-money laundering or terrorist financing requirements.

AML act should be as a measure of prevention to those who are contemplating criminal activity. This deterrence should be intended to prevent a re-offence by the offender by imposing a punishment that money a launderer wouldn't want to experience again. The aim is also to deter others in the community from committing the same or a similar offence by making an example of the offender. Undoubtedly, the enacted laws regarding Anti money laundering will have different consequences
depending upon Legal punishment. In other words, increasing the effectiveness of legal punishment could have a positive effect on successes of AML Laws. For instance: In India, the Punishment prescribed for the offence of ML in cases of money obtained from normal crime is rigorous imprisonment for a term which shall not be less than 3 years but which may extend to 7 years and shall also be liable to fine which may extend to five lakh rupees. However, for the proceeds of crime which is involved in ML relates to any offence specified under Paragraph 2 of Part A112 of the Schedule the punishment of rigorous imprisonment of 7 years has to be read as 10 years.

3.6.4 Technology and AML Laws

Rapid developments in financial information, technology and communication has allowed money to move anywhere in the world with speed and ease. This makes the task of combating money-laundering more urgent than ever. Technology is the making, usage and knowledge of tools, techniques, crafts, systems or methods of organization in order to solve a problem or serve some purpose. Anti-money laundering software is a type of computer program used by financial institutions to analyze customer data and detect suspicious transactions. Anti–Money Laundering Technology assist financial institutions and organizations by providing technology services to mitigate the risk associated with money laundering schemes.

Vaithilingam and Nair (2007) examined the trend of the pervasiveness of money laundering in developed and DGCs through an empirical approach and presented and empirical results of Five key factors as influencing the pervasiveness of money laundering in developed and DGCs. One of five key factors is Technology. The argument is that money laundering is more pervasive in DGCs due to inadequacy of ICT infrastructure, such that an increase in ICT infrastructure in DGCs will bring about positive marginal returns, reducing the pervasiveness by instilling a more transparent anti-money laundering process. This suggests money laundering is more prevalent within DGCs because of it is under developed ICT infrastructure and a slight increase in ICT will bring about a positive marginal returns
There is direct relationship between consequences of AML laws with technology. On other word, technology has positive impacts on consequences of AML laws. Not only the growth of technology has helped the common man it has proved also a boon for these ML and DGCs is not an exception to this. Cyber finance is the growing concept in these developing economies. One of the consequences of AML law is the requirement on FIs to know their customers. Knowing one's customers, FIs will often be able to identify unusual or suspicious behavior, including false identities, unusual transactions, changing behavior, or other indicators of laundering. But for institutions with millions of customers and thousands of customer-contact employees, traditional ways of knowing their customers must be supplemented by technology.

Most of the FIs raise employee awareness by providing them with key information on laws, rules, and procedures. But while laws impose increasingly intense data-management and reporting requirements, implemented solutions are still mainly manual, involving employee intervention. Automated monitoring and detection, and the use of available IT solutions, remain very rare in FIs. Straight through processing is still hard to achieve. Effective reporting or blocking of suspicious transactions, as required by the AML regulations, remains an issue in most organizations.

To deal with rising regulatory pressures and complex compliance, banks need flexible and evolutionary AML solutions that will readily adapt to future changes in both money laundering practices and the regulations designed to fight them. Implementing long term, adaptive AML procedures and using the latest intelligent IT technology (auditing, transaction filtering, profiling, blacklist management, etc.) are essential. FIs must improve international coordination and align their processes, technology, and people behind their AML efforts.

Tightening regulations and laws call for significant changes in financial processes, including:

- Control of clients’ identity and transfers (domestic and cross-border)
- Record-keeping of identity verifications and completed transactions
- Internal reporting of suspicious transactions and appointing an AML reporting officer
External noncompliance reporting, to government, regulators, and other organizations

Auditing

FI's' processes and procedures must also comply with local legislation. The US Patriot Act, for instance, prescribes very strict procedures for foreign account follow-up, as well as strict deadlines for answering regulators' requests.

Given the stringency of regulatory requirements, technology is a key enabler for FI's. Today's money laundering techniques make manual detection extremely difficult. Most current manual systems are inadequate, and FI's are being required by regulators to implement robust technological measures. Adaptive and flexible technical solutions are needed to enable necessary upgrades that will meet future regulatory requirements.

Since many FI's worldwide have no adopted measures to counter ML, criminals are on the lookout for countries with either weak or non-existent control mechanisms. This could indicate that presence or absence of an adequate technological infrastructure is viewed as competitive advantage or disadvantage within the developing countries. Therefore, technology and automation have to be implemented at the FI's.
3.7. Notes


3. The UK uses the term “SARs” rather than “STRs” as the Proceeds of Crime Act 2002 requires disclosure of suspicious activity rather than specific transactions, such as arrangements to launder money whether or not any transactions have been conducted.

4. See: http://www.egmontgroup.org/


6. The Bank Secrecy Act of 1970 requires U.S.A. FIs to assist U.S. government agencies to detect and prevent money laundering. Specifically, the act requires FIs to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. It was passed by the Congress of the United States in 1970. The BSA is sometimes referred to as an "anti-money laundering" law ("AML") or jointly as “BSA/AML”. Several anti-money laundering acts, including provisions in title III of the USA PATRIOT Act, have been enacted up to the present to amend the BSA.

7. For more information visit: http://fiuindia.gov.in/

8. The Mission of Federal Bureau of Investigation is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.
9. The mission of the Drug Enforcement Administration (DEA) is to enforce the controlled substances laws and regulations of the United States and bring to the criminal and civil justice system of the United States, or any other competent jurisdiction, those organizations and principal members of organizations, involved in the growing, manufacture, or distribution of controlled substances appearing in or destined for illicit traffic in the United States; and to recommend and support non-enforcement programs aimed at reducing the availability of illicit controlled substances on the domestic and international markets.


11. HIFCA stands for High Intensity Financial Crime Area," these high risk areas were first announced in the 1999 National Money Laundering Strategy and were conceived in the Money Laundering and Financial Crimes Strategy Act of 1998 as a means of concentrating law enforcement efforts at the federal, state, and local levels in high intensity money laundering zones. HIFCAs may be defined geographically or they can also be created to address money laundering in an industry sector, a financial institution, or group of financial institutions.

12. The JTTF concept started in 1979 when the New York City Police Department recognized the value of integrating agencies at multiple levels to defeat an ever-increasing number of bank robberies. From there, JTTFs began playing an important role in thwarting terrorist activities and disrupting potential attacks domestically. The JTTF's mission is to "investigate acts of terrorism that affect the U.S., its interests, property and citizens, including those employed by the U.S. and military personnel overseas." FBI LAW Enforcement Bulletin, The, The FBI Joint Terrorism Task Force officer, Nov, 2008, by: Brig Barker, Steve Fowler.

13. The Asset Forfeiture and Money Laundering Section (AFMLS) provides centralized management for the Department's asset forfeiture program to ensure its integrity and maximize its law enforcement potential, while also providing managerial direction to the Department's components in prosecuting money laundering. The
Section initiates, coordinates, and reviews legislative and policy proposals impacting on the asset forfeiture program and money laundering enforcement agencies.

14. The term “financial institution” is very broadly defined in the BSA (31 USC 5312) to include: Insured banks, Commercial banks or trust companies, Private bankers, Agencies or branches of foreign banks in the U.S., Credit unions, Thrift institutions, Brokers or dealers registered with the SEC, Brokers or dealers in securities or commodities, Investment bankers or investment companies (includes mutual funds and unregistered), Investment companies, Currency exchanges, Issuers, redeemers or cashiers of travelers’ checks, money orders or similar instruments, Operators of a credit card system, Insurance companies, Dealers in precious metals, stones or jewels, Pawnbrokers, Loan or finance companies, Travel agencies, Money services businesses (MSBs), including persons engaged in providing informal remittance, Services, telegraph companies, Businesses engaged in vehicle sales, including automobile, airplane and boat sales, Persons involved in real estate closings and settlements, The U.S. Postal Service, Agencies of the U.S. government or of a state or local government carrying out a duty or power of a listed business, Casinos or gaming establishments (including Indian gaming operations) with an annual gaming revenue of USD 1 million, any business or agency that engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, or a substitute for any activity in which any of the above businesses is authorized to engage, Futures commission merchants, Commodity trading advisors, Commodity pool operators, Investment advisers (Treasury/FinCEN has issued a proposed AML rule determining investment advisers to be financial institutions).

15. The Joint Money Laundering Steering Group (JMLSG) is made up of the leading UK Trade Associations in the Financial Services Industry. Its aim is to promulgate good practice in countering money laundering and to give practical assistance in interpreting the UK Money Laundering Regulations. JMLSG is currently in process of amending its Guidance to reflect the provisions of draft Money Laundering Regulations 2007, which implement the EU Third Money Laundering directive in the UK.
16. The Financial Services Authority (FSA) is an independent non-governmental body, given statutory powers by the Financial Services and Markets Act 2000.

17. HM Revenue & Customs (HMRC) was formed on the 18 April 2005, following the merger of Inland Revenue and HM Customs and Excise Departments.

18. With the Prevention of Money Laundering (Amendment) Act, 2009 (No 21 of 2009) coming into force from June 1, RBI has issued detailed guidelines on Customer Due Diligence (CDD) measures to be made applicable to Politically Exposed Person (PEP) and their family members or close relatives.

19. Payment of the governmental bills and payments made for municipal services less than the applicable designated shall not require any identification process.

20. The Designated Threshold means conversion of the amount of one hundred and fifty million (150.000.000) rials cash or its equivalent into other foreign currencies and valuable commodities.

21. for more information about the FSA visit: http://www.fsa.gov.uk/


23. Available at: http://www.youngand.co.uk/mlr7.pdf

24. The Council for Licensed Conveyancers (CLC) is the regulatory body for Licensed Conveyancers who are qualified specialist property lawyers.

25. A memorandum of understanding (MOU) is a document describing a bilateral or multilateral agreement between parties.