Money laundering, the illegal use of banking and other financial channels to hide the origin and identity of the criminal owner of the money has been with us for decades. Traditionally associated with tax evasion and the Mafia, it was, until the late 1980s, an often neglected problem. It is of growing global concern, however, as the narcotics trade has blossomed and organized crime networks have disposed of the proceeds of their illegal activities.

Money laundering is considered as an offence by all civilised nations. It is one of the biggest threat to society. The United Nations have recognised that a great amount of wealth is generated through organised crime. The dangers of organised crime increasing and extending its tentacles globally have caused much concern to the United Nations and certain countries which were at the receiving end. After the September, 11th terrorist attack in the United States, the war against terrorist funding has taken momentum.

Money Laundering Defined

In its simplest non-legal terms, money laundering is, “the processing of criminal proceeds (profits or other benefits) in order to disguise their illegal origin” (The Financial Action Task Force (FATF). Note that the act of money laundering occurs only after a predicate criminal offence has been committed to generate the criminal proceeds, which in turn need to be laundered to convert them into “legitimate capital”. This transformation process has become a thriving business, albeit quite illegal in most, but not yet all, countries.

Another Definition of Money Laundering

The process of converting cash or other properties which has been derived from criminal activities so as to give it the appearance of having being obtained from a legitimate source. Successful money laundering enable the criminal to:

- Remove or distance themselves from criminal activities from generating the profits.
- Distance profits from the criminal activities.
- Enjoy the benefits of the profits which bring attention to themselves and,
- Reinvest the profits in future criminal activities or in legitimate business.

Stages

Money laundering occurs in three stages. The first is called displacement, which involves physical disposal of the cash, to move it into the financial system. The second stage involves
technique called layering, which requires moving the money around, through and to multiple institutions in different jurisdictions in order to disguise the audit tail and to make the money in effect, disappear. The final stage is called integration, which requires bringing the money back into the mainstream of commerce and investment as legitimate funds.

Actual cash currency in large amounts is heavy. For that reason, it must generally be placed into the financial system to get it back into circulation. Contrary to movie and television lore, US$ 1,000,000 will not fit into a briefcase. For example, US $ 1 Million in US $ 100 bills weighs 22 pounds (10 kilos), US $ 10 Million in US $ 20 bills weighs 1100 pounds (500 kilos); the same amount in US $ 100 bills still weighs 220 pounds (100 kilos). US $ 100 Million in US $ 100 bills weighs 2200 pounds (1000 kilos).

The Washing Cycle

“One. There are three distinct stages to the [money laundering] cycle. The first is immersion, which means consolidation and placement. A drug dealer who amasses 5 million in cash is faced with the Herculean task of putting perhaps as many as a million pieces of paper into the banking system. Unlike the counterfeiter, who needs to get his forged notes into circulation, the launderer is forced to rely on bank accounts, postal orders, traveller’s cheques and other negotiable instruments to funnel the cash into the banking system.

Continuing the metaphor, the second step - known as layering - might also be called heavy soaping. This is where the launderer disassociates his gains from their illicit source. By moving his money between as many accounts as he can - in and out of dummy companies that he’s set up around the world for just this purpose - and relying on bank secrecy and attorney-client privilege to hide his own identity, he deliberately creates a complex web of financial transactions keeping in mind at every step that his main task here is to obliterate any sort of audit trail.

The final stage is in the spin dry - sometimes described as repatriation and integration. This is the point where the washed funds are brought back into circulation, now in the form of clean, and often taxable, income”.

(Excerpted from “The Laundrymen” by Jeffrey Robinson).

How Pervasive is Money Laundering?

Money laundering is said to be the world’s third largest business in terms of value. And it is growing. How big is it? Because of its shadowy character to begin with, no one knows with any degree of certainty. Both the experts and competent authorities have avoided estimating the scope of the practice. Evidence points to a volume of hundreds of billions of US $ per annum. The IMF and the Financial Action Task Force using 1996 statistics now estimate worldwide money laundering to be at a level of between US $ 600 billion to US $ 1.5 trillion. The IMF estimates money laundering to amount to 2 - 5 per cent of the world’s GDP. But to keep this
vast sum in perspective, the New York clearing system alone handles US $ 3.5 trillion in banking and securities transactions on average business day.

In 1998 it was estimated that trade in counterfeit goods amounted to 7 - 9 per cent of world trade, up from about 3 per cent in 1990. The World Trade Organisation (WTO) and ICC calculate that trade in counterfeit goods in 2000 was about US $ 450 billion. The proceeds of trading derived from intellectual property violations must pass through the money laundering systems.

**Fraud**

An important issue is corporate fraud, which often leads to money laundering. Business are subject to fraud through simple and complex deceptions by both insiders - managers, employees, agents, et al. - and outsiders. Being a victim of fraud is embarrassing and expensive and recoveries are limited. On a wider scale, in the information age, fraud can be perpetrated through credit cards, smart cards, stored value cards, e-money, e-commerce, identity theft, etc. Technology helps both the good and the evil.

The element of fraud involved in the deliberate falsification of company accounts by insiders, whether employees or senior management, is a principal concern of corporate governance. These frauds can be the subject of civil or criminal proceedings depending on the individual country. If this falsification is compounded by an effort to launder the funds illegally received, the legal implications can be very serious indeed. In the years 2001 and 2002 a number of massive corporate frauds have been uncovered and caused the collapse of major corporations.

**Money Laundering Techniques**

The experts have noted little difference in the ways that terrorists and other criminals use the financial and other systems to launder money. The methods identified include in each smuggling by couriers or bulk cash shipments; structured transactions, both into and from bank accounts; purchases of money instruments in various forms and movements of funds via the non-bank or underground systems.

The techniques used in money laundering can be broken down into funds channelled through three principal conduits; (a) banking (b) non-bank institutions and (c) non-financial business. Summarized, these channels and their most common laundering techniques are as follows:

**Banking Institutions**

- Large deposits and transfers
- False name accounts
- Accounts of friends, relatives and cronies
• Smurfing (electronic structured transactions of electronic cash)
• Shell and front companies, usually offshore, for layering transactions
• Lawyers, accountants, consultants, trustees, fiduciaries
• Private Investment Corporations (PICs)
• Collection accounts; special name accounts; correspondent and concentration accounts
• Acquisition of compliant banks
• Payable through account
• Loan back arrangements swaps and option
• Telegraphic transfers (TT) (SWIFT)
• Bank drafts, money orders, cashier’s cheque
• Cash deposits and withdrawal
• Smuggling currency in bulk across border
• Traveller’s cheque
• Internet banking and electronic purse accounts and
• Internet shell bank

Non-banking Financial Institutions

• Bureaus de change, exchange offices, casas de cambi
• Money remittance services (giro houses)
• Underground or ‘parallel banking’ “Black Market Peso Exchange”, ‘hawala’, ‘hundi’. ‘feiqian’, chit and chop shops which handle both legal and illegal foreign exchange transactions in India, South and East Asia, the Middle East and Africa
• Single premium insurance products
• Postal services: money orders, packages (for smuggling cash)
Non-financial Businesses or Professions

- Professional facilitators, e.g. lawyers, accountants, financial advisors, notaries, secretarial companies, trustees and other fiduciaries
- Systems based on trust and loyalty (see ‘hawala’ above)
- Real businesses: false invoicing, commingling of legal and illegal money, loan back arrangements, layering of transactions through offshore shell companies and false import/export declaration
- Commercial trade transactions through Free Trade Zone
- Casinos, bookmaking, internet casinos/gambling
- Real estate companies
- Purchase and cross-border delivery of precious metal
- Use of warrants in the metals market. Or
- False insurance claims - ghost ship

In a study by the FATF on money laundering typologies, “gate keepers” such as some lawyers and accountants, were highlighted as the common elements in complex money laundering schemes. Money launderers often target struggling professional practices that are in financial difficulties, as the latter may find it hard to turn away lucrative business, high risk or not. The FATF reports that lawyers are mostly utilized in establishing corporate entities through which money can be laundered by their clients or by providing the use of bank accounts (client accounts).

There are also charities and NGOs established in order to legitimately receive donations that stem for criminal activities and to fund terrorist activities. Some solicitors arrange to hold funds in their clients’ accounts or in an off-shore trust, making the identification of the true beneficiary impossible. Other services offered by lawyers include advising on complex financial transactions and investment schemes. The law firms in question are not expected to become involved, but rather to serve as a shield to give third parties confidence.

Money Laundering and the Internet

It is commonly believed that the internet provides new and undetectable methods of money laundering (“cyber laundering”). However, in essence, the internet is nothing more than a
messaging system. To move money, banks move information by different kinds of messaging systems.

Identifying customers is the primary problem arising from internet usage. Characteristics of internet banking (easy access, depersonalised contact between customer and financial institutions and the speed of electronic transactions) make customer identification and the monitoring of transactions difficult for the authorities.

**Legislation**

While AML laws have been or are being adopted in over 120 countries, no country yet requires its financial institutions to detect money laundering. Realistically, the most they can do is to require that ‘suspicious transactions’ (hard to define) be reported, subject to a plethora of regulations and policies. Despite the pressing need, which is slowly being recognized by nation states, the effectiveness of anti-money laundering laws has been mixed, ie. it is better than having no laws at all, but falls far short of the ideal of strict, fair and universal enforcement with well-knit international cooperation within and between governments, regulatory and supervisory authorities, law enforcement agencies, the judiciary and the private sector. As usual, vigorous enforcement is limited to too few countries.

At a regional level, several organizations have adopted conventions or other agreements to combat terrorism, including regulations concerning money laundering and/or designated laws that solely tackle money laundering. For example: the European Union in November 2001 widened the scope of the original EU money laundering directive in its Second EU Money Laundering Directive (Directive 2001/97/EC) amending Council Directive 91/308/EEC. The Directive requires EU member states to update their national legislation by June 2003. It criminalizes laundering the proceeds of all serious crimes: extends its applicability to a series of non-financial professionals who are believed to offer or provide vital services for criminals (e.g., casinos, bureaux de change, auctioneers, lawyers, notaries, estate agents, fund transporters and dealers in high cost goods); extends the ‘KYC’ record keeping and suspicious transaction reporting requirement to external accountants and auditors, notaries, lawyers and others.

**Other legislative initiatives are:**

- 1998 BIS - Basel Committee on Banking Supervision - Prevention of criminal use of the banking systems for the purpose of money laundering;

- 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime;

- 1992 Resolution of International Organisation of Securities Commission (IOSCCO)

- 2001 Egmont Group of Financial Intelligence Units - Statement of Purpose;

- 2000 & 2002 Wolfsberg Group of Banks - Guidelines
A number of individual countries enacted new legislation on money laundering or extended laws that were already in place. Some did so under pressure by the FATF, others in a voluntary attempt to intensify the fight against terrorist financing.

Examples are:

- **China**: The People’s Bank of China (Central Bank) AML Regulations - effective March 1, 2003.

- **Russia**: established a Committee of Financial Monitoring in November 2001 that will operate as the country’s financial intelligence unit (FIU).
- **Israel**: issued regulations in the identification of and reporting of suspicious transaction and record-keeping for stock exchange members, portfolio managers, insurance companies and provident funds in November, 2001.
- **Philippines**: Anti-Money Laundering Act of 2001;
- **Guatemala**: Act against Money and Asset Laundering 2001;
- **St. Vincent and Grenadines**: Proceeds of Crime and Money Laundering Prevention Act 2001:
- **Canada**: Proceeds of Crime (Money Laundering Act) 2001
- **Bahamas**: Financial and Corporate Services Providers Act 2000, amended 2001

**USA Patriot Act passed by the US Congress, 25 October 2001**

There are seven concepts in the USA Patriot Act which concepts you need to be aware of if you are to continue doing business in the world, or at least if you plan to continue doing business in dollars. The seven are:

1. A legal requirement that the financial institution know their customers

2. An authorization for the Secretary of the Treasury to take steps, or special measures, if he perceives a money-laundering problem in the future

3. Enhanced due diligence for private banking
4. Serious changes for correspondent banking that will affect all of you

5. A near prohibition of shell banks being allowed to use money transmission and other value transmission systems in the United States

6. Inclusion in the statutory schemes of prohibitions against money laundering by brokerage firms, which until now have avoided the worst burden of the war against money laundering, and

7. Authorization for financial institutions to share information.

First the statute requires that financial institutions know their customers. It does not define the term KYC (“Know Your Customer”) but the statute for the first time requires that financial institutions in fact know the identities of the persons for whom they are acting. That is critical, because in tracking terrorists one needs to be able to rely on accurate financial records, and if the identity of the owner of an account, or the person who directs the flow of money is concealed, the trail is broken. Money is power. The anonymous use of money is the anonymous use of power.

The regulations on how to “know your customer” are not going to be exclusive. It will not be enough to fill out a checklist and say “This Bank has complied”. The proof of whether you know your customer will come when law enforcement tries to ascertain who moved a particular sum of money. The question “who?” needs to be answered with a name, not with a well filled out checklist. The people asking the questions believe that they are at war. ‘Whether you agree with them or not they are likely to view a useless answer (one which they cannot follow up) as a violation by your institution of the Patriot Act.

The next section of the law authorizes the Secretary of the Treasury to take ‘special measures’ to fight money laundering when he perceives a problem. These measures can be directed at a country, a geographic area, a financial institution, or a sector of the economy. This is an attempt to create flexibility to deal with new money laundering practices as we become aware of them. Over the years the sophistication of the money launderers for the Colombian drug dealers has increased greatly; law enforcement is constantly several years behind the cutting edge of the new techniques. This section is designed, in part, to speed up the reaction time for law enforcement.

The third area of concern is private banking. The USA Patriot Act requires enhanced due diligence for private bank accounts, and, in a move with which some bank regulators may well not be in agreement, requires serious due diligence in connection with bank accounts of political leaders and their associates. You are aware, from the cases with Marcos, with Abacha, with Mobutu and Suharto and others, that allegations arise from time to time that a man has looted his country. These tend to be supported by such events as the deposit into one bank
account for a salaried Mexican of 500 years salary, totalling $80 Million, ostensibly saved while his brother was President of Mexico.

The fourth subject in the USA Patriot Act is the most important for Asian bankers - the area of correspondent banking. All correspondent banks, as defined, must appoint an agent in the United States for the service of process. The Secretary of the Treasury and the Attorney General are specifically authorised to issue subpoenas for the production of evidence from any correspondent bank using the money transmission facilities of the United States. The evidence that is sought need not ever have been in the United States, nor does the evidence sought have to be about dollar transactions. The reasoning is that if an institution wants to do business in the United States it must be prepared to make evidence available for the prosecution of those who violate our laws.

If a bank chooses to use correspondent facilities in the United States, it agrees to produce evidence in the United States when compelled to do so by subpoena. If, after due notice, a correspondent bank does not produce the required evidence, the US bank which clears for it, on a request from the government, must close the correspondent account within ten days.

All correspondent banks in the United States must have in the United States an agent authorized to accept the service of process. If process is served on them they must comply, regardless of any bank secrecy laws in the jurisdiction in which the accounts are maintained, or else leave the United States.

In addition banks licensed in the United States are now required to make certain that the banks for whom they act as correspondents have adequate internal due diligence procedures so that if subpoenaed they will be not just willing to comply, but be able to do so. The initial verification of that took an enormous amount of work, performed between October 26 and Christmas Day 2001, in large part by bankers who lost friends in the World Trade Centre.

Shell banks are the fifth area to which the PATRIOT Act relates. The law does its best to bar them from the United States, directly or indirectly. By “shell banks” the statute refers to banks with no physical presence anywhere, which may be licensed, but cannot be supervised or regulated because there is no where for the supervisor or regulator to go. Banks based in the USA are forbidden to have shell banks as customers, and are now required to exercise due diligence to make sure that their correspondent banks do not have shell banks as customers, either. That means that shell banks, to do business in the United States, will need to go through at least three levels of correspondent banks, paying multiple sets of fees to move money.

The Patriot Act brings brokerage firms under the coverage of the anti-money laundering laws, by the definition of ‘financial institution’ which it adopts. There are, as yet, some major unanswered questions as to what aspects of the brokerage business will be covered - clearly deposit taking is covered, but what is the liability of firms as regards the identity of clients acting through off-shore hedge funds whose membership is secret? The People, who wrote the rules, are insisting the brokerage industry must be as transparent as the field of correspondent banking. It is worth repeating that Congress intended to make the entire area of
financial services transparent to law enforcement so that money being used to fund terrorists could be traced, and the sources of that money, and the people responsible, identified.

In one section of the law Congress provided that institutions which announced that they were doing it could share information with each other, thus making more transparent to each other whether a transaction was proper or not. The ability to share information cuts the uncertainty about transactions and thereby cuts the effort that compliance officers have to spend, cutting the costs for everyone. As with the other section of law, the purpose is to increase transparency, so that if there is a need to trace funds, they can be traced. Likewise there are sections permitting banks to exchange information about former employees, and the like. Sections setting forth what constitutes adequate identification and the like are also coming into play now some with Treasury regulations, some without.

All business should be wise to be alert to money laundering methods and tactics, For their own protection, businesses should implement AML defences and counter-measures, and install various other forms of protection.

In Sri Lanka there is no legislation to curb anti money laundering activities. There are only certain guide lines from the Central Bank to Licensed Commercial Banks with regard to money laundering activities. It is understood, that a new legislation with regard to anti money laundering has already been drafted and will be presented to the parliament in the near future.

In the draft Act to prohibit money laundering in Sri Lanka there is provision to establish an anti money laundering authority and it stipulates the powers, functions and duties of the AML authority. Section 4 of the draft Act defines the offence of money laundering as follows:

“Any person who receives, possesses, conceals, invests, disposes of, brings into Sri Lanka, transfers out of Sri Lanka or engages in any other manner in any transaction in relation to any property derived or realized directly or indirectly from any unlawful activity or from the proceeds of any unlawful activity, knowing or having reason to believe that such property is derived or realized directly or indirectly from any unlawful activity or the proceeds thereof, shall be guilty of the offence of money laundering and shall on conviction after trial before the High Court be liable to a fine not less than twice the value of the property in respect of which the offence was committed and not more than three times that value or to rigorous imprisonment for a period of not less than five years and not more than twenty years or to both such fine and imprisonment, and shall be liable to have property forfeited”.

FATF the world watch dog on AML activities has revised its forty recommendations at its meeting held in Germany in June this year. These forty recommendations are instructions for financing regulations to reflect new dangers from money laundering by criminal and terrorists groups. The new rules seek tough checks on high risks business areas, such as, correspondent banking, or dealings with persons who have questionable political history. They have also included casinos, real estates agents, dealers in precious metals and stones. Accountants and lawyers should now be subject to money laundering checks.
This meeting also identified smuggling organised crime and trafficking in humans and drugs as also offences contributing to the offence of money laundering.

The FATF forty recommendations were initially compiled in 1990 and were revised in 1996. Now FATF have again revised the forty recommendations. It also agreed on certain international best practices on combating illicit money transfers where under-ground banks operate internet cafes, travel agencies and export import companies. These were seen as major channels through which terrorists transfer money.

The forty recommendations are divided into four major categories. They are:

1. Legal Systems
2. Measures to be taken by financial institutions and non financial businesses and professions to prevent money laundering and terrorists financing
3. Institutional and other measures, necessary in systems for combating money laundering and terrorists money laundering
4. International co-operation

Money laundering methods and techniques change in response to developing counter measures. The FATF has observed increasingly sophisticated combination of techniques, such as the increased use of legal persons to disguise the true ownership and control illegal proceeds and an increased use of professionals to provide advice and assistance in laundering criminal funds. The FATF calls upon all countries to take necessary steps to bring their national systems for combating money laundering and terrorist financing into compliance with the new FATF recommendations and to effectively implement these measures.

The FATF has eight special recommendations on terrorist financing. Recognising the vital importance of taking action to combat the financing of terrorism it has set out the basic frame work to detect, prevent and suppress the financing of terrorism and terrorist acts. They are:

1. Ratification and implementation of UN instruments

Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

11. Criminalising the financing of terrorism and associated money laundering
Each country should criminalise the financing of terrorism, terrorist acts and terrorist organisations. Countries should ensure that such offences are designated as money laundering predicate offences.

111. Freezing and confiscating terrorist assets

Each country should implement measures to freeze without delay funds or other assets of terrorists, of those who finance terrorism and terrorist organisations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.

Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property, that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations.

V. Reporting suspicious transactions related to terrorism

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used, for terrorism, terrorist acts or by terrorist organisations, they should be required to report promptly their suspicious to the competent authorities.

V. International co-operation

Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organisations. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals.

V1. Alternative remittance

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, are licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions.
V11. Wire transfers

Countries should take measures to require financial institutions, including money remitters to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.

Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of an monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).

V111. Non-profit organisations

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable and countries should ensure that they cannot be misused:

(i) by terrorist organisations posing as legitimate entities;

(ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and

(iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

The Financial Institutions in Sri Lanka will have to adhere to the forty recommendations of the FATF on money laundering and the 8 recommendations on terrorist financing to prevent Sri Lanka being considered as a country which facilitates money laundering and terrorist financing. Once the new legislation on money laundering and terrorist financing is passed in Parliament, any breach or non-observance of the laws will make the Institutions as well as their Board of Directors liable to prosecution.

Mr M Kiritharan

Mr. M. Kiritharan is the Chief Legal Officer, Bank of Ceylon. He is a Solicitor, Attorney-at-Law & Notary Public and holds a Diploma in Business Administration, University of Colombo.

Mr Kiritharan has more than 25 years experience in the filed of Banking and Banking Law and has attended training programmes, Conferences and Workshops in Australia, Italy, Singapore and Thailand. He was a Chief Examiner in the Institute of Bankers - Sri Lanka and President of the Association of Corporate Lawyers of Sri Lanka, Member of the Bar Council of the Bar Association, member, Law Committee of the Sri Lanka Banks’ Association and a Visiting Lecturer in Banking Law in several Institutions.