IMPLICATIONS OF ANTI -MONEY LAUNDERING LEGISLATION –SALIENT FEATURES

By Prasanna Kannangara

Head of Compliance, DFCC Vardhana Bank

1) Financial Action Task Force (FATF)

In 1989 at the G7 Summit the Financial Action Task Force (FATF) which is an inter governmental body was established with the objective of Prevention of Money Laundering (Anti Money Laundering – AML) and Combating Financing Terrorism (CFT). FATF has 34 member states currently (with India obtaining membership in June 2010) and 2 regional organizations with many Associate Members, Regional Bodies and Other International organizations affiliated to it.

The FATF in accordance with their objectives have made 40 recommendations and 9 special recommendations in order to combat Money Laundering.

Asia/Pacific Group (APG) on Money Laundering which was constituted in 1997 is one of the Associate Members of the FATF of which Sri Lanka is one of its founder members.

In order to comply with the FATF recommendations Sri Lanka has evolved three statutory acts relating to Know Your Customer (KYC) (see para 5 below), AML (see para 5 below) and CFT which are as follows.

a) Convention on the Suppression of Terrorist Financing Act (STFA) No.25 of 2005 in relation to CFT
b) Financial Transactions Reporting Act (FTRA) No. 6 of 2006
c) Prevention of Money Laundering Act (PMLA) No.5 of 2006

Financial Intelligence Unit (FIU) is the policing body of above acts as per the FTRA with wide ranging powers.

What is Money Laundering

Money Laundering is where funds generated from "unlawfully activities" i.e. dirty money is deposited in the banking system thereby making it legitimate funds, via concealment of the criminal source of funds.

Set out below are two definitions of Money Laundering
a) FATF

"The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money Laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance as it enables the criminal to enjoy these profits without jeopardizing their sources."

b) The Statutory definition of the Offence of Money Laundering as per the PMLA.S 3(1)

"Any person who engages directly or indirectly in any transaction in relation to any property which is derived or realized directly or indirectly from any "unlawful activity" or from proceeds of any "unlawful activity", or receives, possesses, conceals, ,disposes of, or brings into Sri Lanka, transfers out of Sri Lanka, or invests in Sri Lanka, any property which is 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 from the proceeds of any "unlawful activity", shall be guilty of the offence of money laundering....."

"Unlawful Activity" is defined below at para 3.

As per financing of terrorism is concerned, funds may be received which are generated from lawful activities as well ie from individuals and businesses etc. (see para 6 below)

3) What is "Unlawful Activities" defined by the FTRA and PMLA

As per FTRA and PMLA of 2006, the statutory definition "unlawful activity" relates to any funds generated from or for any one or more of the following

a) the Poisons, Opium and Dangerous Drugs Ordinance (Chapter 218)
b) any law or regulation for the time being in force relating to the prevention and suppression of terrorism (Convention or the Suppression of Terrorist Financing Act No. 25 of 2005)
c) the Bribery Act (Chapter 26)
d) the Firearms Ordinance (Chapter 182), the Explosives Ordinance (Chapter 183) or the Offensive Weapons Act No. 18 of 1966.
e) The Exchange Control Act (Chapter 423)
f) an offence under section 83c of the Banking Act. No. 30 of 1988 (Pyramid Scheme)
g) any law for the time being in force relating to transnational organized crime.
h) any law for the time being in force relating to cyber crime
i) any law for the time being in force relating to offences against children
j) any law for the time being in force relating to offences connected with the trafficking of persons and

k) an offence under any other law for the time being in force which is punishable by death or with imprisonment for a term of seven years or more.

Clause k) is an "omnibus" clause intended to incorporate all other acts, which may not be covered in above definition

Hence person/persons or entities which directly or indirectly deal with funds generated from above "unlawful activities" (as defined above in para 3) will be guilty of an offense of "Money Laundering" as per the PMLA and as per CFT is concerned the funds collected either lawfully or unlawfully are applied for an "unlawful activity" ie terrorism.

4) Stages of Money Laundering

There are three stages of Money Laundering as follows.

Placement	Funds generated from any "Unlawful Activity" entering the banking system by deposit to a Bank account
Layering	Funds entering the banking system as per above being moved around i.e. transferred, and retransferred many times through various accounts within the bank or outside the bank until its origin cannot be traced
Investment	Funds involved in layering above being integrated into the legitimate economy via purchase of property, gold, jewellery, paintings etc

5) Some steps taken by Financial Institutions to prevent Money Laundering

KYC	• Identity of customer i.e. establish that the potential customer is the person who he claims to be • verify address of potential customer
AML	• Economic Profile including estimated activity in the account which should reconcile to his legitimate earning • Introductions by an existing customer or reputed person • Monitoring of account against estimated activities • Report any suspicious transactions which is in variance with estimated activity of the account per the economic profile of customer or other types of suspicious transaction to FIU • Reporting of statutory cash & electronic transactions over Rs. 1M (currently at August 2010) on a two weekly basis to FIU • Training of staff on KYC, AML, statutory acts and on recognition and reporting of suspicious transactions

6) STFA- An Overview

S 3 (1)

States that any person who unlawfully and willfully provides or collects funds knowing that it would be or likely to be used in terrorist activities as described in Schedule 1 (includes 10 conventions) in the STFA or any other act which may cause death, injury etc. shall be guilty of the offence of financing of terrorist or terrorist organizations.

The STFA differs from the PMLA and FTRA in that the funds collected may not necessarily originate from "unlawful activity" (though quite often that is the case ie from illegal drug trade etc) but provided willfully with the knowledge that it would be utilized to finance terrorism which is an "unlawful activity".

S 3 (2)

Any person who attempts to commit, "aides or abets" the commission of above or acts with one or more persons on above will be guilty of an offence under this act.

In such instance the Bank by opening an account where terrorist related monies are deposited can be held to be "aiding and abetting" terrorism. Thus the Bank has to exercise care and carry out its KYC procedures with diligence to ensure that such funds are not deposited in the banking system.

S 3 (3)

> Where S 3 (1) or (2) is committed by a body of person, then every member, Director, Manager, Secretary, Officer or servant will be guilty of an offence under the act unless it can be proved that they were not aware of the offence or that they exercised due diligence to prevent such an offence

Hence it would seem that if a Bank has "aided and abetted" above terrorist funds to be deposited, all those responsible in the Bank will be personally guilty of said offence and would be liable for punishment as set out below under s 3(4)..

S 3 (4)

Punishment for above offence is not less than fifteen years and not more than twenty years imprisonment and also be liable to a fine.

7) PMLA- An Overview

- Section 3(2)

> Persons who attempts or conspires to commit the offence of money laundering, or aids and abets the commission of money laundering shall be guilty of the offence of money laundering.

Same as in STFA S3(2) but has the added wording of "or conspires" . In such instance the Bank by opening an account and accepting "unlawfully" generated monies as deposits can be held to be "aiding and abetting" such activity. Thus the Bank has to exercise care and carry out its KYC procedures with diligence to ensure that such funds are not deposited in the banking system.

Punishment for contravention for above two S 3(1)(re accepting funds generated from "unlawful activity" see para 2(c) above) & 3(2) is fines in between the value of property in respect of which an offence is committed and not more than three times its value or not less than 5 years and not exceeding 20 years rigorous imprisonment or both.

- S 4

  It must be deemed/presumed that any movable or immovable property has been acquired by a person via "unlawful activity" until the contrary is proved ie that he had known income etc to match such property

What this states is that at first instance it must be deemed/presumed that any person with money and property has obtained it from "unlawful activities" as defined in the PMLA and FTRA until or unless it can be demonstrated that the person has obtained such money and property from "lawfully activities" i.e. via inheritance, business profits, salary etc. to match such money and property.

- S 5

  Any person who has information obtained by him through the engagement of his vocation, that any property has been derived or realized from any illegal activity, shall (notwithstanding the existence of secrecy provisions-S 5 (4) in various laws) disclose such information to the Financial Intelligence Unit (FIU). Failure to provide information (without reasonable grounds for non disclosure) shall be an offence

For example a Credit Officer in a bank may examine an credit application form and become aware via visits etc that the movable and immovable property belonging to an individual could not have been obtained from his lawfully generated funds or has been generated from funds from "unlawful activities". As the Officer has become aware of this while "engaging in his vocation" he has to report this situation to the FIU.

- S 6

  Any person who knowing that an investigation into Money Laundering has commenced or is about to commence, divulges such information (other than for purpose of carrying out a duty under the Act) to any person knowing that such disclosure would prejudice the investigation, or disclosures the identity of the person who is being investigated, or knowingly falsifies, conceals or destroys any material relevant to the investigation commits an offence.

Punishment for contravention of S 5 & 6 is fines not exceeding Rs.50,000 or imprisonment not exceeding 6 months or both.

- S 7 & 8 Freezing Orders

  A Police Officer (SP and above-if SP not available ASP) may make an order prohibiting any transaction in relation to any account, property or investment, which may have been used, is being used or may be used in relation to

money laundering. Such order shall be initially valid up to 7 days. The order to be valid has to be confirmed by the High Court who can extend it for a further period of time. HC can permit essential transactions to be made. Such confirmation issued by the HC can be extended for up to 1 year. If indictment is filed prior to expiry of 1 year, the order shall be in force till the conclusion of the trial. If convicted the order shall be in force until the determination of the Appeal. Transactions in contravention of a Freezing Order, shall be null and void. HC may appoint a 'Receiver' to deal with the property during the operational period of the Freezing Order.

Punishment for contravention S 7 & 8 is fines not exceeding Rs.100,000 or one and a half times the value of the money in the account which ever is higher or imprisonment not exceeding one year or both.

8) FTRA- An Overview

The FTRA statutorily deals with the KYC and AML requirements, the main sections of which is set out below. Para 5 above in general fits into the sections set out below

- Know Your Customer S 2
  The above process relates to identification of persons who wish to open an account with the bank by establishing that the said person is the individual he/she claims to be As per section 2(3) of the FTRA on 18.5.07 the FIU issued rules on identifying documents required to be taken by banks, including for verification of address

- Maintenance of Records S 4
  From the closure of account or cessation of business relationship all identifying documents per section 2 above must be kept by the bank for a period of six years. This also applies to all reports, records transaction details furnished to FIU

- Due Diligence and Scrutiny of Customers S 5(a) & (b)
  This relates to monitoring of activity of account to ensure that it is consistent with bank's knowledge of business profile and source of funds

- Customer Profile Building S 5(b)
  The financial profile on all monitory aspects pertaining to customer including estimated activity on the account i.e. estimated deposits etc.

- Customer Risk Profile S 5(b)
  Asses the risk posed by the customer and risk categorise customer to assist in the monitoring process

- Report Transactions to FIU S 6

  Report all cash and electronic fund transfers over Rs.1 M (at August 2010)to FIU on a two weekly basis

- Reporting Suspicious Transactions S 7 & 8

  Report to FIU all "Suspicious Transactions" or attempted transactions related to any "unlawful activity" or any other criminal offence.

- Non-Disclosure of Reporting to FIU S 9 & 10

  All transactions reported to FIU under sections 6,7 & 8 not to be disclosed to any other person

- Staff Protection S 12 (1)

  No civil criminal on disciplinary action can be taken against an institution, an auditor or supervising authority of that institution, a director, partner, an officer, employee of an institution or agent acting on behalf of that institution who complies with the terms of the Act in "good faith".

- S 14 (1) Every Institution shall be required to ;

  (a) appoint a Compliance Officer who shall be responsible for ensuring the Institution's compliance with the requirements of the FTRA.

  (b) establish and maintain procedures and systems to ;

  i) implement the customer identification requirements under S 2.
  ii) implement procedures for the record keeping and retention requirements under S 4.
  iii) implement the process of monitoring required under S 5 (re-account activity etc on an "on going" basis)
  iv) implement the reporting requirements under S 6,7,8 (to FIU) and section 22 in relation to auditors.
  v) make its officers and employees aware of the laws relating to money laundering and financing of terrorism and.
  vi) screen all persons before hiring them as employees.

  (c) establish an audit function to test its procedures and systems for the compliance with the provisions of this Act.

  (d) train its officers, employees and agents to recognize suspicious transaction.

- Examples of Suspicious Transactions

  - Inconsistencies in account opening documents i.e. name and or/address differs on NIC and utility bill.
  - Defensive reactions to questions asked by the bank i.e. on inconsistent documents, purpose for which the account is to be opened etc.
  - Insist on opening account with copy documents and unable/unwilling to provide originals.
  - Residence of customers differs to the location at which he is attempting to open the account
  - Shared address with another customer with no relationship
  - Trying to open account on a non-face to face basis
  - Opening account on a non-face to face basis from abroad but unwilling to forward original documents.
  - False or forged account opening documents
  - Clubs, NGOs, Trust etc. trying to open account but reluctant to provide information of beneficiaries, controlling parties etc.
  - One large foreign inward remittance with multiple foreign outward remittances and vice versa.
  - Many transfers to and from other accounts
  - Exchange of small denomination notes (Rs50, Rs 100 and Rs 200) for large denomination notes (Rs1,000,Rs 2,000)
  - Movements of very large amounts of cash by a customer with no legitimate source;
  - use of unusually large amounts in trave ler's cheques/Foreign Currency
  - OTC large cash transactions buying T/Cs, Foreign currency, FDs etc
  - Amounts that seem large in the context of that particular customer.
  - Use of multiple accounts without a acceptable reason
  - Many transactions i.e. deposits and withdrawals below the FTRA reporting requirement limit of Rs.1 M (as at August 2010) and above pertaining to cash and
    all electronic fund transfers.
  - Activity in accounts takes place at a branch geographically displaced from that of the residence of the customer.
  - Majority of activity approx. 80% in account in on a cash basis.
  - Transactions in account inconsistent with customer's known profile
  - Any transactions done with countries not strong on Anti Money Laundering or with
    black listed countries/tax heavens
  - Round sum transactions not in line with business transaction
  - Sudden surge of activity in the account especially after change of address etc.
  - Dormant account activated but no transaction for a period of time
  - Customer unconcerned about changes and commission levied by the bank

- Regular third party deposits to the account especially on accounts of students and housewives.
- non-activity of salary account opened by a company for its staff
- Loan collaterised by cash
- Customer attempting to settle NPA loan with no reasonable explanation as to source of funds etc.
- Early settlement of loan with cash.
- Customer unconcerned about terms of loan, interest rates, charges etc.
- Caution to be exercised on Bill of Lading issued by a Freight Forwarders or NVOCCs as opposed to that issued by Shipping Liner itself.
- Regular price variances of goods(imported/exported) – inflated prices of goods as compared to the market
- Important information of LC missing (name & address of applicant, beneficiary details, name and address of issuing/advising bank, description of goods, nature and number of documents)

- Imposition of Penalty To Enforce Compliance with FTRA

S 19(1)

For person who is required to conform to the Act and who fails to do so will be liable for a

- Penalty not exceeding Rs. 1 Mn
- Double the penalty for continuing non-compliance on each occasion thereafter.

S 19(5)

Directors, General Manager, Secretary on other similar officers of the bank have personal liability of above amounts unless he is able to prove he was not aware of the non-compliance or that he exercised due diligence to ensure compliance.

S 19(4)

Additional measures may be taken by supervisory authorities, regulatory bodies i.e. Banking License could be cancelled.

S 19(6)

FIU may direct adoption of measures to ensure compliance

Part VI of the FTRA S 28 (6) states

"A person who opens, operates or authorizes the opening or the operation of an account with an Institution in a fictitious or false name is guilty of an offence and shall be punishable on conviction to a fine not exceeding one hundred thousand rupees or imprisonment of either description for a term not exceeding one year, or to both such fine and imprisonment."

This has a direct impact on the staff who open accounts, authorisers the opening of a account or operations of an account for customers on whom KYC has not been done correctly which could result in above set out punishments.

It would seem from above that if one authorises the operation of a account in a fictitious name he would be liable to above penalties even though he may not have been responsible for the opening of the account.

9) Information to be Collected from Potential Customers

In relation FATF 40 recommendations and 9 special recommendations plus the three statutory acts STFA,FTRA and PMLA, the FIU issued a Direction dated 18.5.07 relating to "Rules On Customer Due Diligence For Financial Institutions And Non Bank *Financial Institutions" which states among other matters*

Maintenance of Accounts:
Para 2

"The general customer information to be recorded at the outset should include customer's business/profession, level of income, economic profile, business associates and other connections, source of funds, and the purpose for which the account is opened."

The above information is obtained after the basic verification of name, address etc is carried out by the bank.

Further the said FIU Direction states that banks are required to obtain the following information for each of below set out types of organizations. Thus KYC information is required on all Individuals, Partners of partnerships, Directors of Limited Liability Companies, Trustees of Trust etc. who wish to open an account with the Ban

Proprietorship/Partnership Accounts:

- Personal details of the proprietor/partners as in the case of individual accounts

Corporations/Limited Liability Company:

- Personal details of all Directors as in the case of individual customers.

Clubs, Societies, Charities, Associations and NGOs:

- Customer information form as in the case of individual accounts.

Trust, nominees, and fiduciary accounts:

- Identification of all trustees, settlers/grantors and beneficiaries in case of trustees.

Under said FIU Direction of 18.7.07 per Part 11 –Specific Guidance all financial institutions are required to comply with the following when opening accounts for individuals.

- Full name as appearing in the identification document.
- Identification document to be specified as, national identity card, unexpired passport, official driving license.
- Permanent address as appearing on the identification document. Any other address to be accepted should be supported by a utility bill not over three months old. Utility bills are to be specified as electricity bill, water bill and telecom or any fixed line operator's bill. No post-box number should be accepted. In the case of 'C/o', property owner's consent and other relevant address verification documents are required to be obtained.
- Telephone number, fax number, and e-mail address.
- Nationality
- Occupation, business, public position held and the name of the employer.
- Purpose for which the account is opened.
- Expected turnover/volume of business.
- The reason for choosing to open the account in a foreign jurisdiction in case of NRFC/ NRRAs.
- Satisfactory reference.
- Signature

Documents to be obtained (each copy should be duly certified by the authority issuing same)

- Mandate/Account Opening form
- Copy of identification document.
- Copy of address verification documents.
- Copy of the valid visa/permit in the case of RNNFC/NRRA/RGFC accounts for non-nationals.
- Business registration if the account is opened for such purpose.

Hence the AML/KYC account opening forms have been designed in such a manner that above information can be obtained from customers prior to commencement of the banking relationship, including the estimated deposits to be made monthly which is matched against the actual deposits made to the account and material variances investigated in compliance with S5 of the FTRA re "Ongoing Due Diligence and Scrutiny of Customers". The estimated deposits to the account is to be reviewed at least once a year or more often which is dependant on the individual customer's changing circumstances and risk profile.

10) Customer Information Requested by Banks on their Respective AML Forms

Based on above requirements at para 9) above the following are the some of the main areas information requested by Banks on their respective AML/KYC forms besides the basic information as set out in FIU direction of 18.5.07 i.e. relating to the establishment of name ,address verification and salary/commission/consultancy fees details etc.

i) Wealth & Estimated Value for individuals

ii) Source of Wealth for individuals

iii) Other Connected Businesses

iv) Purpose of Opening Account & Usage

v) Status of residential address (owner occupied, rented etc)

vi) Source of funds for business accounts

vii) Indicate in brief the principal nature of activity in the case of business account

viii) Anticipated volumes of deposits on account

ix) Assets owned by Business

x) Source of assets owned by Business

Wealth & Estimated Value and Source of Wealth

Obtaining of above from a practical view point would not be easy .However if detail of customer's wealth is not obtained how does the bank ascertain his "economic profile"? (see para 9 above). Funds generated by his assets in addition to any other "lawfully" earned money ie salary etc should be in line with customer's wealth(and "source of wealth").This would provide the bank with a reasonable understanding of his financial standing and the reasonableness of the intended deposits to the account. If this is not done the bank will have to accept customer's word on the deposits to be made to his account per month without any reality (and run the risk of customer laundering money via the bank account), unless the bank can be satisfied of the "source of funds".

The above information assists the bank to ascertain to a large extend (on the assumption that bank is satisfied that the basic information is realistic) that customer will not be generating and depositing funds from unknown sources i.e. from "unlawful activities" per PML & FTRA of 2006. Hence at very minimal customer declaration as evidenced by his signature must be obtained

on the AML account opening forms plus the "wealth" details. At end of day the bank should satisfy themselves of the customer's financial standing and that he/ the organization is lawfully capable of generating the claimed deposit levels of funds to his account.

It is appreciated that customers may not give accurate figures on above due to many reasons. However the bank will have to re-examine this factor once the account becomes operational at least once a year(with high risk customers more often) by matching the deposits to the account to the estimated deposits with a view to ascertaining that funds are not being laundered via the account especially on high risk customers and re-adjusting the customer profile.

If the customer commences depositing money over and above the original estimated funds after the account was opened, the bank has to inquire from where the funds are originating as it would seem that he is not capable of generating such levels of income from his known sources of income (on the assumption that the bank has carried out the statutory KYC procedures.) The pending AML software will carry out above task of matching expected deposits with actuals and provide exception and "suspicious transaction" reports, as this task cannot be done manually due to the volume of transactions involved and the number of customers of a bank.

Funds deposited over and above that originally estimated may be from legitimate sources. The Bank's Compliance Officer will have to make a decision and perhaps report it on a Suspicious Transaction Report (STR) to FIU if there are grounds to do so. Customers may well have sold a vehicle etc. and hence deposits a large cash sum and if the bank is satisfied that such is the case no STR is required to be sent to the FIU.

If the FIU does ascertain from outside sources (which has happened often in the past) that a customer has been involved in depositing funds obtained from and/or for (terrorism) "unlawfully activities" in bank accounts and the bank has not reported it on a STR to FIU due to the lack of the basic KYC checks carried out as per the above Acts & FIU direction i.e. not obtained details his wealth and source of wealth etc. inquiries may be made by FIU to ascertain if bank has been carrying out all the statutory procedures or if the Bank/staff have been deliberately or negligently "adding and abating" (section 3(2) of PML 2006) Money Laundering. If this is the case penalties in various forms may ensue including possible jail sentences for staff responsible beside the "reputational risk" to the Bank and contravention of FIU direction of 18.5.07 .

In above situations did the banks involved not realize that funds deposited by above mentioned persons and companies possibly originate from "unlawful activities"? Did the banks concerned not "Know Your Customer" (KYC) i.e. not carry out sufficient checks to ensure financial standing of above referred individuals and companies and realize that from the known information of his wealth and income generated etc that such monies could not have been lawfully generated by such a persons?

If the bank had not carried out their statutory KYC checks on the customers it may not have been in a position to detect the possibility that these customers were not capable of "lawfully earning" monies that they had been depositing and hence opening the door to Money Laundering,

11) Correspondent Bank (NOSTRO) AML Questionnaire and Related Issues

Correspondent banks annually require certification that all AML procedures (in line with International Standard of FATF 40 recommendations and 9 special recommendations and the Wolfsberg AML Principles) are in place in the bank.

The three Sri Lankan AML acts mirror above standard as stated at para 1 above . If the Compliance Officer is unable to provide a signed certificate on compliance with AML Acts as the requirements of said Acts are not in place in the Bank, the correspondent bank is unlikely to allow operations on the NOSTRO account with obvious negative effects on the Bank's foreign trade finance business.

Further if the authorities (Secretary of Treasury) in the USA are of the view that a foreign bank is laundering funds through a NOSTRO account in the USA (funds having been generated for example from the narcotics trade, internet gambling proceeds, terrorist funding or from other "unlawful activities" via inward/outward remittances, foreign cheque/draft collections etc), as per USA PATRIOT ACT 2001 section 319 Secretary of Treasury has the power to instruct the offending bank to forfeit the funds in the NOSTRO account.

In connection with above all the bank's customers should be screened against a international sanctions list ie "WorldCheck" etc. to ensure that known money launderers and terrorist especially foreign individuals do not obtain access to banking system. In addition the bank has to ensure that transactions are not carried out with jurisdictions which are black listed i.e. Burma, Sudan, North Korea etc.

CONCLUSION

Hence as per above it is vital that the framework on AML per the acts are established within the bank and executed on a on-going basis. As Financial Institutions, we need to ensure the enforcement of these Acts and Directions are implemented equally and completely. The tools and the regulatory guidance provided ensure that Financial Institutions are able to verify a customer's identity and their transactions to ensure money is not laundered via the legitimate banking system. Thus, it is in the interest of the financial institution to combat money laundering and terrorist financing in order to avoid regulatory, litigation and reputation risk while being a socially responsible citizen.