I. INTRODUCTION

Money laundering and those who engage in it have gone global and “pose a serious threat worldwide in terms of national and international security, as well as political, economic, financial and social disruptions.”\(^1\) It is a formidable problem for the international community, a new form of geopolitics and one of the most pernicious forms of criminality of which the dimensions have yet to be fully measured and the impact fully determined.\(^2\)

Since money laundering is the processing of the criminal proceeds to conceal their illegal origin, the objective of the launderer is to disguise the illicit origin of the substantial profits generated by the criminal activity so that such profits can be used as if they were derived from a legitimate source.\(^3\)

It appears to be accepted that there are three phases or stages in the laundering process. The first is the placement, where cash enters the financial system. This is the choke point or the nerve center of the procedure, where the launderer is more vulnerable and the attempt to launder can easily be identified. The second stage is the layering where the money is involved in a number of transactions so that the tracing of the origin of the money is lost. Finally the third stage is integration, where money is mixed with lawful funds or integrated back into the economy, with the appearance of legitimacy. The thrust of this report is on the important first stage.

\(^2\) See Report of the Secretary-General, 4 April 1996 at p.4; UN Press Release SOC/CP/179 20 May 1996; UNCPJ Newsletter nos. 30/31, Dec 1995 at p.5.
\(^3\) Countering Money Laundering: The FATF, The European Union and the Portuguese Experiences - Past and Current Developments, Dr. Gil Galvao - Paper presented at 117th International Senior Seminar, UNAFEI, Tokyo, at p.1.
markets, it is not sufficient to have domestic measures to combat money laundering. It is paramount therefore that action against money laundering and measures to prevent it are universally applied.\(^5\)

In 1988, the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention) was adopted and the incrimination of money laundering was included in an international treaty for the first time.

A. Financial Action Task Force

The Financial Action Task Force\(^6\) (FATF) was founded in 1989 by the G-7 Summit in Paris to examine ways to combat money laundering. It published a report in 1990 with forty Recommendations\(^7\) which were to become the standard by which anti-money laundering measures should be judged. In 1996 the recommendations were revised to reflect the changes which have occurred in the money laundering problem.

The relevant provisions within the broad ambit of intelligence are recommendations 10-12, 14, 15, 19, 21-25, 28 and 29 respectively.\(^8\)

B. Egmont Group of Financial Intelligence Units\(^9\) (Egmont Group)

Following the FATF Recommendations several countries put in place legislation to counter money laundering and established their Finance Intelligence Units (FIU). The Egmont Group which comprises of the FIUs’ of the world, defined an FIU as

“A central national agency responsible for receiving (and, as permitted, requesting), analyzing and disseminating to the present authorities, disclosures of financial information

(i) concerning suspected proceeds of crime, or

(ii) required by national legislation or regulation,

in order to counter money laundering.”\(^10\)

\(^4\) The United States criminalized money laundering on October 27, 1986 by passing the Money Laundering Control Act of 1986.

\(^5\) See Footnote 3, supra, at p.5.

\(^6\) The FATF currently consists of 26 countries and two international organizations. Its membership includes the major financial center countries of Europe, North America and Asia. It is a multi-disciplinary body - as is essential in dealing with money laundering - bringing together the policymaking power of legal, financial and law enforcement experts.

\(^7\) The forty recommendations set out the basic framework for anti-money laundering efforts and they are designed to be of universal application. They cover the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation.

\(^8\) For the full text of these recommendations please see appendix 1.

\(^9\) The Egmont Group meetings named after the Egmont-Arenburg palace in Brussels on April 1995, consists of countries that have operational Financial Units. The group currently consists of 53 countries including: Aruba, Australia, Austria, Belgium, Bermuda, Bolivia, Brazil, British Virgin Islands, Bulgaria, Chile, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Finland France, Greece, Guernsey, Hong Kong, Hungary, Iceland, Ireland, Isle of Man, Italy, Japan, Jersey, Latvia, Lithuania, Luxembourg, Mexico, Monaco, Netherlands, NL Antilles, New Zealand, Norway, Panama, Paraguay, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Taiwan, Turkey, United Kingdom, United States, Venezuela.

\(^10\) This definition was adopted at the plenary meeting of the Egmont Group in Rome in November 1996 and reaffirmed in the Madrid meeting.
In its statement of purpose\textsuperscript{11} the Egmont Group, among other things, recognized the international nature of money laundering and realized that many governments have both imposed disclosure obligations on financial institutions and designated FIU’s to receive, analyze and disseminate to competent authorities such disclosures of financial information. It is also increase the effectiveness of individual FIUs and contribute to the success of the global fight against money laundering.

The 18 countries represented in this seminar have different legal stages in combating money laundering and establishment of FIUs. A majority has draft proposals for legislation against money laundering. Countries such as Fiji, South Africa and Tanzania have legislation but short of an independent FIU although in each of these countries suspicious transaction reports (STRs) are either made to the police or the Director of Public Prosecution (DPP) by Financial Institutions and/or by persons conducting a business or who are in charge of a business undertaking.

C. UN Convention against TOC
In November 2000, United Nations Convention against Transnational Organized Crime was adopted by the United Nations General Assembly and it was opened for signature by member states in December 2000. It requires member countries among other things, as follows:

“Article 7, Paragraph 1
Each State Party:
(a) Shall institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions ... which regime shall emphasize requirements for customer identification, record-keeping and the reporting of suspicious transactions;
(b) ... shall consider the establishment of a financial intelligence unit to serve as a national center for the collection, analysis and dissemination of information regarding potential money-laundering.”

D. Techniques of “Placement” of Illicit Funds into the Financial System
We submit that it is important in this report to identify the various techniques money launderers utilize the financial system to launder their money.

1. The Banking Sector
(i) Banks remain an important mechanism for the disposal of criminal proceeds, though there appears to be a recognition by money launderers that obvious techniques such as depositing large sums of cash into bank accounts for subsequent transfer is likely to be reported to law enforcement authorities, and thus extra steps are being taken. The technique of “smurfing” or “structuring” was commonly used - this technique entails making numerous deposits of small amounts below a reporting threshold, usually to a large number of accounts.

(ii) Accounts in false names or accounts held in the name of relatives, associates or other persons operating on behalf of the criminal. Other methods used to hide the beneficial owner of the property include the use of shell companies.

\textsuperscript{11} Resolved in Madrid on 24 June 1997.
(iii) Use of “collection account”. Immigrants from foreign countries would pay many small amounts into one account and the money would then be sent abroad. Often the foreign account would receive payments from a number of apparently unconnected accounts in the source country.

(iv) Use of “payable through accounts”. These are demand deposits account maintained at financial institutions by foreign banks or corporations. The foreign bank funnels all the deposits and cheques of it’s customers into one account that the foreign bank holds at the local bank. The foreign customers have signatory authority to the account as sub-account holders and can conduct normal international banking activities. The payable through accounts pose challenge to “know your customer” policies and STR guidelines.

(v) Loan back arrangements in conjunction with cash smuggling. By this technique, the launderer usually transfers the illegal proceeds to another country, and then deposit the proceeds as a security or guarantee for a bank loan, which is then sent back to the original country. This method not only gives the laundered money the appearance of a genuine loan but also often provides tax advantages.

(vi) Telegraphic transfers, bank drafts, money orders and cashier’s cheques are common instruments for money laundering.

2. Non-Bank Financial Institutions

Banks offer a wide range of financial products and hold the largest share of the financial market and accordingly the services they provide are widely used for money laundering. However, non-bank financial institutions and non-financial businesses are becoming more attractive avenues for introducing ill-gotten gains into regular financial channels as the anti money laundering regulations in the banking sector becomes increasingly effective. The channels used include:

(i) Bureau de change, exchange offices or casa de cambio. They offer a range of services which are attractive to criminals such as:

(ii) Exchange services which can be used to buy or sell foreign currencies, as well as consolidating small denomination bank notes into larger ones;

(iii) Exchanging financial instruments such as traveler’s cheques; and

(iv) Telegraphic transfer facilities.

(v) Remittance services.

(vi) Use of hawala, hundi or so called “underground banking”.

3. Non-Financial Businesses or Professions

(i) These include lawyers, accountants, financial advisors, notaries, secretarial companies and other fiduciaries whose services are employed to assist in the disposal of criminal profits.

(ii) Casinos and other businesses associated with gambling.

(iii) Purchase and cross border delivery
II. METHODS OF OBTAINING INTELLIGENCE

A. STR System

The objective of an STR system is to facilitate the detection of illicit proceeds of crime as it enters the financial system via the financial institutions, i.e., at the placement stage of the money laundering process. This is the “choke point” where money laundering is most vulnerable. It is important therefore that a legal checks and balance system is put in place to

(i) legally recognize the STR system domestically in compliance with the FATF recommendations;
(ii) exert obligatory compliance by financial institutions to the STR provisions;
(iii) sanction non-compliance by financial institutions of the legal STR obligations; and
(iv) safeguard the integrity of the financial system.  

This requires a methodical and practical approach to the form of STR relevant to suit a given situation in each jurisdiction. For instance, the form of STR expected from a financial institution would vary from a law or accountant firm due to the nature of the transactions peculiar to them.

In this report we propose to examine the STR of financial institutions and briefly the FIU of Japan and a comparative glimpse of Hong Kong and the United States as well.

1. The Japanese STR System and FIU

In 1992, the STR system was first introduced into Japanese legislation by the enactment of the Anti-Drug Special Law. Subsequent to this, the Anti-Organized Crime Law was enacted in year 2000 which introduced a comprehensive STR system. The scope of predicate offence of money laundering was expanded to almost all organized crimes. Based on the law, the Japan Financial Intelligence Office (JAFIO) was established in the Financial Services Agency (FSA) as the Japanese Financial Intelligence Unit.

12 A typical example is the BCCI (The Bank of Credit and Commerce International) case. Unlike any ordinary bank, BCCI was from its earliest days made up of multiplying layers of entities, related to one another through an impenetrable series of holding companies, affiliates, subsidiaries, banks-within-banks, insider dealings and nominee relationships. By fracturing corporate structure, record keeping, regulatory review, and audits, the complex BCCI family of entities was able to evade ordinary legal restrictions on the movement of capital and goods as a matter of daily practice and routine. Thus it becomes an ideal mechanism for facilitating illicit activity by others, including many governments’ officials whose laws BCCI was breaking.

BCCI’s criminality included fraud by BCCI and BCCI customers involving billions of dollars; money laundering in Europe, Africa, Asia, and the Americas; and use of shell corporations. BCCI’s bribery of officials in most of those locations; support of terrorism, arms trafficking, and the sale of nuclear technologies; management of prostitution; the commission and facilitation of income tax evasion, smuggling, and illegal immigration; illicit purchases of banks and real estate and a panoply of financial crimes limited only by the imagination of its officers and customers.

It is important to note also that among BCCI’s principal mechanisms (techniques) for committing crimes are that which we noted at item 1.4 above.

13 See Appendix 4 for the guidelines issued by the Monetary Authority of Hong Kong to financial institutions for the prevention of money laundering.

14 See Appendix 2 & 3 for the standard form of STRs by financial institutions and the full text of a typical STR in Japan.
At present, depository institutions (banks), insurance companies, securities brokers and other non-bank financial institutions are covered in the STR system. However, non-financial institutions or other relevant professionals (so called gatekeepers) are not covered. Compliance by financial institutions is mandatory but no legal sanction is provided for non-disclosure of STRs.

B. Better quality STRs vis a vis Know Your Customer Policy and Rules

In order to facilitate better quality and reliable suspicious transaction reports banks and other financial institutions should know their customers.

What does that mean?
(i) Making every reasonable effort to determine the true identity and beneficial ownership of the accounts.
(ii) Knowing the source of the funds.
(iii) Knowing the nature of the customers business.
(iv) Knowing what constitute reasonable account activity.

Why are bankers concerned?
(i) Can they simply take people at face value?
(ii) Who are they dealing with?
(iii) Where do they come from?
(iv) How do we prove this information accurate?
(v) Where are we dealing with them?
(vi) Why should we bother?

Why cannot they simply take people at face value?

Unfortunately, quite a lot of people are not honest. The net result could be a bad debt or fraud. More importantly being involved with criminals puts their reputation at risk.
Therefore, it could be said that identification is rarely certain and difficult to prove. This statement would also be true in relation to the place of residence or domicile. Thus the way ahead is closer partnership to reduce difficulties.

C. Recommended Guidelines for STRs

In the context of the report, the following guidelines are recommended.

1. Cash Transactions

(i) Large deposits and withdrawals without rational reasons.

(ii) Transactions frequently made in short periods of time and accompanied by large deposits and withdrawals without rational reasons.

(iii) Transactions where large amounts of small-denomination coins or bills without rational reasons.

(iv) Large cash deposits into night safe facilities or rapid increase of amount without rational reasons.

2. Opening of New Accounts

(i) New accounts in fictitious names or in the name of other persons.

(ii) Accounts that are suspected of having been opened in fictitious names or in the names of other persons.

(iii) Accounts bearing the names of corporations that are suspected of never having existed.

(iv) Customers who wish to have cash cards sent to destinations other than their addresses.

(v) Customers who have tried to open accounts by mail-order without proper information.

(vi) Customers who attempt to open multiple accounts without rational reasons.

(vii) Customers who have no convincing reasons to make transactions at a particular branch.

3. Transactions through Existing Accounts

(i) Accounts that have been used for large deposits and withdrawals during a short period of time after their opening and have then been closed or discontinued for any other transactions without rational reasons.

(ii) Transactions where large deposits and withdrawals are made frequently without rational reasons.

(iii) Accounts with frequent remittances to a large number of people without rational reasons.

(iv) Accounts that customers use for receiving frequent remittances from a large number of people without rational reasons.

(v) Accounts that have not been active for a long time and suddenly experiences large deposits and withdrawals without rational reasons.

(vi) Transactions those are unusual from the viewpoint of economic rationality.

4. Trading in Bonds and/or Other Securities

(i) Transactions where customers bring in large amounts of bonds and/or other securities to sell them for cash without rational reasons.

(ii) Customers settle trading in bonds and/or other securities with checks drawn by/or remittances from third parties without rational reasons.

(iii) Customers attempting to buy large amounts of bonds for cash or checks and then request to receive bond certificates while refusing to use depositary services without rational reasons.
5. **Transactions Related to Safekeeping Deposit and Safety Boxes**

   (i) Customers use safety box facilities frequently without rational reasons.

6. **Cross-border Transactions**

   (i) Customers who provide information which is suspected of being falsified or ambiguous information.

   (ii) Customers make frequent large overseas remittances within short periods of time without rational reasons.

   (iii) Customers send large overseas remittances for economically unreasonable purposes.

   (iv) Customers receive large remittances from abroad that are economically unreasonable.

   (v) Customers frequently order or encash large amounts of traveler's or remittance checks without rational reasons.

   (vi) Customers who are based in jurisdictions which do not cooperate with international anti-money laundering efforts or are shipping illegal drugs.

   (vii) Customers carry out with parties based in NCCTs (Non-Cooperative Countries and Territories\(^{15}\)) or jurisdictions which are shipping illegal drugs.

   (viii) Customers introduced by parties based in NCCTs or jurisdictions which are shipping illegal drugs.

7. **Loan Transactions**

   (i) Customers unexpectedly make repayments of overdue loan.

   (ii) Loan applications where borrowing customers put up assets held by third parties as collateral.

8. **Other Transactions**

   (i) Customers who jointly visit a bank branch and request different tellers to make large cash or foreign exchange deals.

   (ii) Customers who refuse to explain reasons or submit information when requested to verify the intended beneficiary.

   (iii) Transactions that are made by employees of banks or their relatives to benefit parties that are unknown.

   (iv) Transactions where employees of banks are suspected of committing crimes.

   (v) Transactions where deposits are made with forged or stolen money or securities and the customers are suspected of knowing that the money or securities are forged or stolen.

   (vi) Customers who unusually emphasize the secrecy of the deals, and customers who attempt to ask, force or bribe bank officials.

   (vii) Transactions that are identified as unusual by bank officials based on their knowledge and previous experience, and transactions involving customers whose attitudes or actions are identified as unusual by bank officials.

**III. OTHER METHODS OF INTELLIGENCE\(^{16}\)**

Apart from STRs detected through the financial institutions, there are other methods of intelligence to detect money laundering offences. These include:

---

\(^{15}\) These are countries identified by FATF to have insufficient laws and regulations to assist in the fight against money laundering.

\(^{16}\) Some of the methods mentioned in this sub topic are also canvassed by Group 3 in their report.
A. Private Informers

The use of private informers could serve as a useful source of intelligence in money laundering investigations. However, one should expect the perils of using private informers as a source of intelligence in investigation. It is most prudent if possible to maintain the anonymity of these informers. The disclosure of their identity and the nature of information may risk the truth seeking mission of the criminal justice systems in using rewarded criminals as witnesses.

B. Surveillance (Electronic/Cyber)

Interception of private communication is a commonly used method of intelligence gathering. The use of electronic devices and computers feature a common tool in these operations. The use of persons in surveillance could also be described as another means in this regard. The wire tap as it is commonly known may not be recognized as a legitimate source of intelligence in certain jurisdiction however it is believed to be used widely as a source of intelligence gathering in investigation.

C. Undercover Operations

The courts have long upheld the validity of undercover operations as a means of intelligence gathering in investigation. The conduct of personnel in this operation must be that which does not violate fundamental fairness and does not impeach the fundamental rights of individuals.

D. Information derived from a Criminal Investigation

This source is derived through interrogation. The usage of interrogation in criminal investigation would in certain instances serve to alert the investigator about sources that target intelligence in regard to other crime. No one person is likely to know the full extent of criminal enterprise. Therefore these interviews of different persons in criminal investigation could contribute as a source of intelligence gathering with regard to further criminal activity.

IV. PROBLEMS IN THE FUNCTIONING OF FINANCIAL UNIT AND PROPOSED SOLUTIONS

Financial Intelligence Units are functioning in some countries like United States of America, Japan, Hong Kong, etc. envisaged in their statutes to combat money laundering. Various problems have been experienced in it's functioning to make it a potent weapon against this crime. Money laundering has become a global phenomenon with the help of modern technology and it needs a global effort to combat it. Some major problems to fight this menace are enumerated here.

A. Lack of Relevant Legislation to Criminalize Money Laundering

A number of countries do not have the legislation to criminalize money laundering. All such countries need to make enactments in this connection to make this global effort successful. International pressure also needs to be brought on such countries to take immediate steps in this direction.

B. Absence of FIU

Some countries have the legislation to fight against money laundering but they have not created FIU. Fiji is an example where money laundering legislation exists but there is no FIU to build financial intelligence system. Such countries need to create FIUs expeditiously suitable to their situation in order to fight money laundering effectively.

---

17 As in the Operation Casablanca case.
C. Limited Scope of FIU

There are countries like Japan which have the required legislation and FIU but their STRs are limited to only banks and financial institutions. Transactions relating to real-estate, luxury cars, jewelers are not covered. In some countries, post-offices also conduct financial transactions just like banks. Real estate transactions are made through lawyers and attorneys. A significant part of illegal money is laundered through real-estate transactions. Similarly accountants, money-changers, businesses and trades can also be required to submit STRs to FIU to broaden the scope of FIU and facilitate analysis. Each country can think of broadening the scope of FIU according to its situation and requirement.

D. Improper Analysis of STRs

In most cases, receiving the STRs from banks and financial institutions without other relevant information about the transaction and proper analysis does not serve a useful purpose in identifying and detecting that the transaction relates to money-laundering. FIUs need to have access to wider data-bases of enforcement agencies like police, anti drug-trafficking enforcement agencies, anti-corruption agencies, customs and income-tax departments in order to analyze the STRs meaningfully.

The system of submission of STRs to FIUs and analysis by FIUs need to be computerized with the help of suitable software to make the job of analysis meaningful. Sometimes it may be necessary for analysis purposes to have additional information about the nature of the transaction and the persons involved in the transaction. For this purpose, FIU should have the authority to access further information from banks, financial institutions and law enforcement authorities.

E. Quality of STRs

Banks and financial institutions may find it difficult to identify as to which transaction is suspicious and which is not. In an attempt to overcome this difficulty, for instance, the USA has adopted the threshold approach in addition to STR system. Their legislation provides that cash transactions of $10,000 and above should be reported to the FIU and the concept of Currency Transaction Report (CTR) was introduced. This approach results in receiving large number of CTRs which makes the process of identifying a suspicious transaction and analysis difficult. However, an accessible database was created for law enforcement authorities.18

In the case of Costa Rica, record keeping by financial institutions in a prescribed form is also undertaken on a threshold basis for access by law enforcement authorities when necessary.

Another approach may be proper education and training of personnel of banks and financial institutions in identifying suspicious transactions. Countries like Japan and Hong Kong have issued detailed guidelines to banks and financial institutions as to which transactions are to be suspected. There is also a necessity of monitoring banks and financial institutions and ensuring that they comply with instructions and guidelines regarding submission of STRs. In Hong Kong, a bank official has been designated as a compliance officer who monitors that guidelines are enforced. The experience has been found to be useful and can be useful for adoption by other countries.

18 The Financial Crimes Enforcement Network (FinCEN) is the US FIU. It has a large data base that is accessible by law enforcement authorities and likewise, FinCEN can access their data bases.
F. Absence of Sanctions for Non-Disclosure of STRs

The provision of sanctions for non-compliance of guidelines to submit STRs by banks and other financial institutions need to be made in the relevant statute. Some countries do not have any criminal sanction for non-compliance. Each country should provide appropriate sanction for non-compliance in its legislation.

G. Extension of STRs to Non-Financial Institutions

STRs need to be broad based in order to fight money laundering. It has been found in countries where legal provisions for mandatory reporting to FIU exist that money launderers have turned to alternative avenues of money laundering due to tightening of controls in financial sectors. Legal provisions can be made to bring in the gatekeepers (lawyers and accountants), tax advisors, real-estate agents, dealers in high value goods and casinos etc. requiring them to file STRs.

Gate-keeper is a new anti-money laundering jargon and defined as someone who is responsible for allowing someone else access to a field although he does not own the gate or the field. They provide several services that may open the “gate” to financial transactions, management of deposits or securities accounts, real-estate transactions, investment services, company formation, creation of trusts and financial and tax-advice. This is a delicate and controversial issue and a balanced approach needs to be adopted reconciling requirements of professional secrecy and fight against money laundering.

The dividing line may be ascertaining the legal position for a client or representing a client in a legal proceeding and participation in a financial transaction involving money laundering. Here again, the problem of identification of a particular transaction being suspicious by persons and institutions may arise. The solution may be found either in threshold approach or public education and awareness. It will depend on each country to adopt a particular approach or a combination according to its own conditions.

The European Union had brought in a directive in 1991 making STRs by financial institutions mandatory which came into effect in 1993. It has now brought an amendment to this directive in the year 2000 that the above-mentioned gatekeepers, business and trade-institutions should also be brought in the ambit of mandatory reporting of suspicious transactions.

In addition to STR, the USA also has provisions of filing CTR by casinos and Internal Revenue Service (IRS 8300) by trades and businesses. A Currency Monetary Instrument Report (CMIR) is required to be filed to customs authorities whenever money is transported in or out of the country.

V. CONCLUSION

It should be noted that a good number of jurisdictions do not have anti-money laundering legislation and do not have a Financial Intelligence Unit system. They should be encouraged to enact legislation in this contest and take constructive measures to set up suitable Financial Intelligence Units.

The jurisdictions who possess necessary legislation to tackle the laundering problem should identify and be mindful of deficiencies money in their systems and take appropriate measures to remedy the situation.

It would also be appropriate to suggest that suitable public awareness programmes
be set up to educate both official and the general public in the sensitivities to the working of the anti-money laundering system.

Relevant jurisdictions should also take note of all matters discussed above and adopt appropriate recommendations with regard to the solutions discussed.