The Latest in Financial and Economic Crimes: Issues involved and Policy Responses

Wassim Shahin*

INTRODUCTION

Hegel's dialectic or the triad consisting of a thesis, an antithesis, and a synthesis can best describe in my opinion the dynamics among financial and economic criminals on one hand, and domestic and international regulators, organizations and conventions on the other. While regulators are satisfied with enforcing and improving existing laws and regulations constituting the "thesis", financial and economic criminals are after developing new modes of crimes for the purpose of, simply stated, profits and gains. These new criminal modes and techniques become the "antithesis". The new laws and regulations developed to face this antithesis form the "synthesis" which becomes the "new thesis". This new thesis makes regulators satisfied that crimes are abated as the cycle of criminal activities decreases from its previous antithesis peak to a trough. However, cycles reach a low to be followed by another peak as substitution into new modes of crimes develops with criminals coming-up with new ideas to regain ill-gotten profits forming the new antithesis to be followed by a synthesis which becomes another new thesis. Technological developments help both sides but more the criminals as they exploit them to strengthen their antithesis as happened with cyberspace crimes and terrorism. The moral of the dialectic is that there would always be financial and economic crimes with regulations lagging behind just because profits lead ethics and laws. A pessimistic statement or optimistic for some is that at best, regulators can increase the slope of the cycle reducing criminal activities faster and extend the periodicity of the cycle keeping economic and financial crimes at their low level longer before the trough starts increasing again to new criminal high levels. Determining whether the glass is half-empty or half-full depends on whether one is drinking or pouring.

The literature on the theory and practice of economic and financial crimes has addressed and is still covering topics that are central to the policy responses aimed at combatting criminal, corrupt, fraudulent, terrorist-financing and money laundering activities. The oldest, largest and most important forum covering these topics and addressing the policies aimed at combatting them is the "International Symposium on Economic Crime" organized by the University of Cambridge for the last thirty-one consecutive years. Viewing the coverage of the last three years reveals that the twenty-ninth symposium of

2011 was entitled “Responsibility for Risk”, the thirtieth symposium of 2012 had a theme of “Economic Crime-Surviving the Fall, the Myths and Realities”, whereas the thirty-first symposium of 2013 had a title of “Fighting Economic Crime in the Modern World: the Role of the Private Sector-Partners and Problems”.

Even though the International symposium has different focus every year, there exists a body of common topics reflecting the most important criminal issues and the internationally accepted and recommended methods in preventing and controlling the economically motivated crimes. The issues covered in seminars and workshops as well as the country application cases amount to over fifty. However, every session includes around twelve different presentations amounting to hundreds of different studies with varying approaches, analysis, results and policy implications over each symposium let alone the three year coverage. I will confine my analysis to practically all major issues addressed in the last three symposia except the country application ones while combining matching issues into the same categories for a total of fifteen groups of one or several issues each. The analysis is thus completely mine as I only relied on the topics in the symposia to back my choice of topics making the paper motivated by the issues discussed there. I will follow an alphabetical coverage of topics researched from the most reliable sources of bodies specialized in the combatting of economic and financial crimes providing some examples and cases where relevant.

TOPICS IN FINANCIAL AND ECONOMIC CRIMES AND POLICY RESPONSES

1. AML/CFT/COMPLIANCE/RISK BASED APPROACH

The Financial Action Task Force on the laundering of money (FATF) has redefined its mission to include, in addition to the combatting of money laundering and countering the financing of terrorism (AML/CFT), the financing of proliferation of weapons of mass destruction. Thus, it developed in February 2012 40 new recommendations to replace the 40 + 9 ones and de-emphasized its 25 criteria. The requirements have been strengthened in higher risk areas and in areas where implementation could be enhanced and made more flexible in low risk areas based on the new risk based approach (RBA). They have become also tougher on corruption and clearer on transparency. The revised recommendations include a new specific one on the proliferation of weapons of mass destruction as recommendation 7. The financing of terrorism is incorporated in the body of the 40 recommendations (recommendations 5 and 6) instead of being covered in the additional nine special recommendations. Equally important is the introduction of the RBA as the first recommendation. This approach ties and maps the strength of the

adopted measures to the risk of the areas involved by ensuring that measures to prevent money laundering and terrorist financing are commensurate with the risks identified in each area for more efficient allocation of country resources across the AML/CFT parlance. Thus, clearly stated, countries should ensure that their AML/CFT regime adequately addresses identified higher risks. Simplified measures may be used for identified lower risks for some of the FATF Recommendations under certain conditions.

The proliferation of weapons of mass destruction or financing proliferation will be addressed in its special relevant section. This section will address recommendations 5 and 6 on CFT that summarize the previous additional 9 recommendations related to terrorism in the old framework. Recommendation 5 states that countries should criminalize terrorist financing, financing of terrorist organizations and individual terrorists and ensure that such offences belong to the money laundering scheme. Recommendation 6 deals with the implementation of financial sanctions in compliance with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The resolutions require to freeze the funds or other assets and to ensure that no funds or other assets are made available to the parties accused under recommendation 5.

As a result of these 40 new recommendations, FATF developed a list of 33 jurisdictions as of 18 October 2013 that are either subject to counter-measures by the international regulatory bodies, or ones that have not made sufficient progress in addressing the deficiencies in AML/CFT or ones that have only recently provided high level of political commitment to address deficiencies. A report by the US Treasury Financial Crime Enforcement Network (FinCEN) on September 17, 2013 confirmed the previous standings of June 21, 2013.

.

Countries and jurisdictions not complying with some or more of the 40 recommendations where found deficient in the following strategic AML/CFT areas: (1) adequately criminalizing money laundering and terrorist financing; (2) establishing and implementing an adequate legal framework for identifying, tracing and freezing terrorist assets; (3) implementing an adequate AML/CFT supervisory and oversight program for all financial sectors; (4) establishing and implementing adequate procedures for confiscation of assets related to money laundering and other terrorist activities; (5) establishing a fully operational, autonomous and effectively functioning Financial Intelligence Unit (FIU); (6) establishing and implementing effective controls for cross-border cash transactions; (7) enhancing the framework for international co-operation related to terrorist financing; (8) ensuring that appropriate laws and procedures are in place to provide mutual legal assistance; (9) addressing secrecy provisions; (10) ensuring an effective supervisory program for AML/CFT compliance; (11) improving suspicious

transaction reporting requirements; (12) ensuring comprehensive and effective customer due diligence measures and record-keeping requirements;

Thus, compliance in the following areas and other ones related to the specific stipulations of each recommendation is necessary for the removal from the list of countries and jurisdictions with AML/CFT deficiencies. In this spirit and as part of its on-going review of compliance with the AML/CFT standards, the FATF has identified as per a statement on October 18, 2013 19 jurisdictions suffering from strategic AML/CFT deficiencies for which they have developed an action plan with the FATF (in addition to the other 14 jurisdictions with AML/CFT deficiencies). While the situations differ among each jurisdiction, each jurisdiction has provided a written high-level political commitment and action plan to address the identified deficiencies.

As an application to the compliance with AML/CFT procedures, the following country case is highlighted. Lebanon, which is excluded from the FATF and the FinCEN lists of countries and jurisdictions with AML/CFT deficiencies has been highly cooperating with the FATF 40 new recommendations. As additional evidence to its total commitment to international norms, the Lebanese Government approved in the middle of March 2012 three important laws proposed by the Ministry of Finance (see Shahin 2013). They include an amendment of the law on fighting money laundering (number 318/2001), declaring of cross-border money transfers, and exchanging tax information. The government enlarged the scope of Law 318 to include most financial crimes and the protection of intellectual property. It has enlarged the obligation of AML reporting to new categories and sectors (property developers, lawyers, and others) and modified procedures in order to make the work of the Special Investigation Commission (SIC) more efficient. Most of the amendments are in line with commitments made within the framework of the FATF's new recommendations. The government included in the bill of cross-borders money transfers a definition of money which includes in addition to cash, other means of transactional payment such as commercial debentures and financial paper. The government cited, as necessitating causes for the new law, the need for effective participation in the efforts of the international community in fighting money laundering and the financing of terrorism. This law was also passed to meet the ninth FATF recommendation stating that every government should take measures to track cross-border cash transfer going in and out.

2. ASSET RECOVERY/POLITICALLY EXPOSED PERSONS (PEPs)

Asset recovery refers to attempts made by individual countries and jurisdictions, international organizations such as the World Bank and the United Nations to recover stolen assets largely from developing countries once these assets have left their home. It is estimated that $20-$40 billion is lost every year in developing countries through

corruption alone and the proceeds of all type of crimes in the global economy are estimated to represent between $ 1 trillion and $ 1.6 trillion annually with half coming from developing countries (see Stephenson, et.al., 2011). Given the large amount of stolen funds through acts of bribery, corruption, embezzlement, theft and other criminal activities by high-ranking officials and leaders and their close associates, the United Nations Office on Drugs and Crime (UNODC) and the World Bank initiated the Stolen Asset Recovery (StAR) Initiative in 2007 to assist countries to locate and return their stolen funds largely hidden abroad in outside countries and jurisdictions mostly enjoying some type of financial secrecy and lax regulatory environments. StAR estimates that only $ 5 billion in stolen funds have been repatriated to the country of origin over the last 15 years. Thus, StAR's work does not only cover locating and returning assets to home countries as it would like to seek international cooperation from all regulatory bodies in developing measures to identify and trace stolen assets, in preventing assets from leaving victim jurisdictions and from entering financial centers abroad. Thus, the process of asset recovery starts at home to prevent assets from leaving and continues through a sequence of identifying-tracing-restraining-confiscating-repatriating stolen wealth.

An important measure aimed at preventing assets from leaving the country of origin is the FATF recommendation 4 on confiscation and provisional measures. It states that countries should develop measures to enable their competent authorities to freeze or seize and confiscate ill-gotten properties and proceeds. Countries should consider adopting measures that allow such proceeds to be confiscated without requiring a criminal conviction, or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

Another measure to prevent stolen funds from leaving the country of origin or from being hidden abroad is through developing guidance on politically exposed persons (PEP's) reflected in FATF recommendations 12 and 22. Thus, in June 2013, FATF developed a paper entitled **"**Guidance on Politically Exposed Persons" to assist countries and the private sector in the development and implementation of measures to implement recommendations 12 and 22. The crux of these measures is that, in addition to performing normal customer due diligence, financial institutions should be required, in relation to foreign PEPs to have appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP; to obtain senior management approval for establishing or continuing such business relationships; to take reasonable measures to establish the source of wealth and source of funds; and conduct enhanced ongoing monitoring of the business relationship. Additionally, financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. The requirements for all types of PEP should

also apply to family members or close associates of such PEPs. The recovery of stolen assets has been enhanced by various international bodies such as in the development of the United Nations Convention against Corruption (UNCAC). This convention requires signatories to assist countries and jurisdictions that have been victims of corruption by freezing, confiscating and repatriating any proceeds of corruption deposited in their jurisdictions.

Despite all of these international attempts several barriers remain significant to asset recovery. The StAR initiative lists and analyzes these barriers as follows (see Stephenson, et.al., 2011). First, general barriers in the form of lack of trust among parties involved in asset recovery, lack of a comprehensive asset recovery policy, deficient resources as originating and requested jurisdictions often do not commit sufficient resources to assist in asset recovery cases, lack of adherence to and enforcement of AML/CFT measures, and lack of effective coordination among involved parties. Second, legal barriers and requirements that delay assistance such as differences in legal traditions, inability to provide formal mutual legal assistance in criminal and asset recovery cases, failure to observe and criminalize all offences listed in the United Nations Convention against Corruption (UNCAC) and the United Nations Convention against Transnational Organized Crime (UNTOC), unbalanced notice requirements that allow dissipation of assets, financial secrecy laws, lack of non-conviction based confiscation mechanism as specified in FATF recommendation 12, inability to enter into plea agreements by many jurisdictions out of concern that the truth-finding process will be distorted, immunity laws that prevent prosecution and mutual legal assistance, inability to recognize and enforce foreign confiscation and restraint orders, and finally the inability to return assets to originating jurisdictions. Third, some operational barriers and communication issues such as the absence or ambiguous focal points of contact between originating and requesting jurisdictions, lack of information on mutual legal assistance requirements, unreasonable delay in responses, identifying foreign bank accounts, and lack of publicly available registries for properties.

3. CORRUPTION/BRIBERY/FRAUD

The issues of corruption, bribery and fraud have been termed as “the enemy within” where penetration of firms by illegal practices take effect. These practices constitute a risk for financial institutions and an encouragement to conduct money laundering to clean the proceeds of these illegal activities. Thus, the topics discussed under this heading can in addition to the risk and money laundering take the form of the perimeters of corruption in the business world, its trend in the literature on criminology, the strategic importance of corruption as a cause of revolutions, the boundaries of corruption, the possibility of legitimate influence becoming corruption, corruption and fraud using internet

intelligence, securities and insurance fraud, elderly and the socially vulnerable victims of financial fraud among many other topics (International Symposium on economic crime, 2011-2013). Fighting corruption, bribery and fraud can take place within the firm through proper governance and audit known as "policing from inside" or through government and international initiatives. Examples are found in the Inter-American Convention against Corruption, adopted in March 1996 by the Organization of American States as one of the first multilateral anticorruption agreements, the "US Foreign Corrupt Practices Act", the "UK Bribery Act", the "UK Serious Fraud Office" the "United Nations Convention against Corruption (UNCAC)", United Nations Office on Drugs and Crime (UNODC), the "G20 Anti-Corruption Working Group (ACWG)", as well as various FATF initiatives aimed at preventing the laundering of the proceeds of crime.

The FATF had developed since 2011 several documents to address the issue of corruption and its impact on the AML/CFT recommendations. Specifically, in July 2011, a report on "Laundering the Proceeds of Corruption" was developed to address typologies used for this purpose. Cases were analyzed from a practitioner's perspective to assist in the understanding of money laundering techniques used. In June 2012, a report on "Specific Risk Factors in Laundering the Proceeds of Corruption: Assistance to Reporting Entities" was written to provide assistance to financial institutions and designated non-financial businesses and profession (DNFBPs) to better analyze and understand the specific risk factors associated with laundering the proceeds of corruption. In October 2012, the document entitled "A Reference Guide and Information Note on the use of the FATF Recommendations to support the fight against Corruption (the Corruption Information Note)" was published. This note was aimed at the general public to explain how to leverage AML/CFT measures in the fight against corruption.

According to the FATF various reports on corruption especially the Best Practices Paper of October 18, 2013, "The Use of the FATF Recommendations to Combat Corruption", it was stated that the G20 called upon the FATF to address the problem of corruption as part of its work on combating money laundering and terrorist financing. Corruption and money laundering are linked in the sense that the proceeds of fraud, corruption and bribery need to be concealed and cleaned. It is true that the FATF Recommendations were designed to combat money laundering and terrorist financing. However, they can serve to combat corruption by protecting private sector institutions from criminal abuse, increasing transparency of the financial system and facilitating the detection, investigation and prosecution of corruption and money laundering.

In the Best Practices paper, it was reiterated that the FATF has held on February 2011, October 2012 and 2013 three experts meetings, jointly with the G20 Anti-Corruption Working Group (ACWG), to provide an international platform for the exchange of views between AML/CFT and Anti-Corruption experts. It was agreed that there was a need for

further tools to enhance the understanding of the FATF Recommendations to use them more effectively in the fight against corruption.

4. CYBER-CRIME/INFORMATION TECHNOLOGY

Cyber terrorism has become the fifth domain of warfare after land, sea, air and space. Cyber -attacks and threats start with simple cyber individual hacking, wire fraud, credit card fraud, network penetration, cyber espionage, organized crime, nation state cyber-attacks or cyber terrorism. Governments, financial organizations as well as other groups in society have been penetrated lately by cyber-criminals. Thus, several threats of cyber-terrorism have been associated with many historic battles. US secretary of defense Leon Panetta has been quoted as saying that the next Pearl Harbor is a cyber-attack. Cyber-space attacks have been called an electronic Chernobyl, a digital Armageddon as well as Trojans from Trojan horse. I would like to add to the literature a term I have coined which is a reverse D-Day where the letter D stands for digital instead of decision and where the term reverse reflects that the bad guys are digitally attacking the good ones. Thus, there is a need to come-up with methods to combat this new type of terrorism.

This new type of terrorism involves rational agents maximizing expected utility based on the occurrence of certain states. I would like thus to rely on the definition of conventional terrorism to define cyber-space terrorism as the threat or actual use of cyber-attacks to attain a financial or political goal. However, cyber-terrorism differs from conventional one in the cost of the terrorist event, the risk where cyber events may be untraceable and harder to track compared to activities requiring physical presence such as skyjacking, the location of the attackers that could be hidden, the impact of the same attack on individuals in different countries (terrorism sans-frontiere), and the ungoverned space or lack of a regulator for cyber-space.

Tow political examples of the last two months can be used to highlight the severity of cyber-attacks. In the Wall Street Journal of Friday, September 27, 2013, Europe Edition, under “Cyber Warfare”, it was stated that U.S. officials said Iran hacked unclassified Navy computers in recent weeks in an escalation of Iranian cyber intrusions targeting the U.S. military. The attacks were carried out by hackers working for Iran's government or by a group acting with the approval of Iranian leaders. The most recent incident came in the week starting Sept. 15, before a security upgrade, the officials said. The allegations would mark one of the most serious infiltrations of U.S. government computer systems by Iran. Previously, Iranian-backed infiltration and surveillance efforts have targeted U.S. banks and computer networks running energy companies, current and former U.S. officials have said.

The second case relates to claims arising on October 23, 2013 that the U.S. National Security Agency (NSA) conducted widespread spying on its European allies including monitoring German Chancellor Angela Merkel's cell phone. According to a CNN report on Saturday October 26, 2013, Merkel said the assertions that the NSA spied on her and other world leaders had "severely shaken" relationships between Europe and the United States, and that trust would have to be rebuilt. Germany and Brazil are drafting a U.N. resolution regarding the protection of privacy in electronic communication. Brazilian and German diplomats met on Thursday to discuss the possible U.N. resolution, government officials in Brazil said. The German spying allegation came in the same week that the French daily newspaper "Le Monde" reported claims that the NSA intercepted more than 70 million phone calls in France over a 30-day period as per the same CNN report.

In a financial case reflecting cyber-attacks from within the organization, a bank in a country in the Arab Gulf witnessed a fraud in its credit cards issuance in May and June 2013 (International Symposium on economic crime, 2013). Around 200 credit cards were issued and sent all over the world to different groups. The trick is that these cards were issued without withdrawal limits which the system read as no limit or infinity. Over $40 million were withdrawn from ATM machines world-wide using these cards. Payments software were changed to repair this issue. The perpetrators fled to a country with no extradition agreements with the Gulf country. On another financial note, HSBC has started changing passwords for employees and customers every 30 seconds if the requested number was not used.

A cartoon in the New York Times summarizes it all by stating: "Believe me, it is so much easier to do it on line". With the Internet becoming more and more prevalent worldwide, commercial websites and Internet payment systems are potentially subject to a wide range of risks and vulnerabilities that can be exploited by criminal organizations and terrorist groups. In this respect, FATF developed in 2008 a report entitled "Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payments Systems". The study analyzed money laundering and terrorist financing (ML/TF) risks associated with commercial websites and Internet payment systems providing case studies. Four main recommendations come-out of the study. The first recommendation is developing guidance mechanisms to detect suspicious transactions. Second, the study aims at making traditional financial institutions aware that they still have an important role to play in the detection and the monitoring of suspicious internet financial transactions. Third, given the international character of the issues at hand, international cooperation is a key factor in the fight against ML and TF including the exchange of information and data pertaining to the criminal misuse of commercial websites and Internet payment systems. Fourth, it is consequently important that all world-wide governments impose regulations requiring customer identification, due diligence, record keeping and transaction reporting, to avoid certain Internet payment

service providers choosing the country with the poorest regulations or one that is not at all regulated.

5. DUE DILIGENCE/KNOW YOUR CUSTOMER/CORRESPONDENT BANKING

The issues of customer due diligence (CDD) and record keeping are the subject of FATF recommendations 10 and 11. Several countries and jurisdictions have been found deficient in applying the requirements stipulated in the two recommendations. As part of its CDD, FATF prohibits financial institutions from keeping anonymous accounts or accounts in obviously fictitious names and requires them to undertake CDD measures when establishing business relations, carrying –out occasional transactions above the applicable threshold or when there is suspicion of money laundering, terrorist financing, the veracity of a customer's identification or the beneficial owner. The principle that financial institutions should conduct CDD should be set out in law or enforceable means depending on specific countries. Additionally, financial institutions should be required to maintain, for at least five years, all necessary records on domestic and international transactions, for proper record keeping and to enable them to comply swiftly with information requests from the competent authorities.

To cite an example of customer due diligence and record keeping, operating banks in Lebanon have been constantly abiding by recommendations 10 and 11. This is reflected in creating at each bank a special department for this task known as compliance unit and in abiding by both the circulars issued by the Central Bank and the Special Investigation Commission (SIC) in this regard, and by the international standards including the US ones of "Know Your Customer (KYC)" to prevent the Lebanese banking sector from being used for illegal or criminal operations. The KYC procedures have been improved over the years and now all customers' names are screened against databases provided by worldwide reputable specialized firms and against local watch-lists provided by the SIC. Customers are required to identify the "source of their funds". Transactions that are inconsistent with the normal line of their businesses and suspected for hiding illegal activities are disclosed and reported to the SIC. It is to mention that the banks' customer data base is segmented into three risk levels in accordance with the risk-based approach formula as included in the local and international best practices, especially FATF, based on the Central Bank of Lebanon circular 190/2010 (see Shahin, 2013).

The relationship with correspondent banks is the subject of recommendation 13. Financial institutions should be required to gather sufficient information about a correspondent institution, assess the correspondent institution's AML/CFT controls,

clearly understand the respective responsibilities of each institution and be satisfied that the correspondent bank has conducted CDD on the customers. In this spirit for example, the Central Bank of Lebanon issued on April 5, 2012, in support of measures practiced by the banking sector, Basic Circular Nb. 126. This circular aims to prevent reputational risks to which Lebanese banks and financial institutions might be exposed to by conducting their operations through subsidiaries or sister companies or by way of correspondents' banks abroad. In addition to other requirements mentioned in this basic circular, the Lebanese banks have to be fully informed of the laws and regulations governing their correspondents' banks abroad, and deal with the latter in conformity with the laws, regulations, procedures, sanctions and restrictions adopted by international legal organizations or by the sovereign authorities in the correspondents' home countries. This circular is applicable to banks operating in Lebanon and their subsidiaries and branches abroad. Thus, Lebanese banks, whether in Lebanon or abroad, are keen on maintaining good and clear relations with correspondent banks. Therefore, they will not undertake any activity in Lebanon or abroad that might expose correspondent banks and jeopardize the relationship with them by involving them in situations contravening the regulations in force in their respective countries.

6. FINANCIAL INCLUSION

The emphasis of FATF on financial inclusion is motivated by the objective of protecting the integrity of the global financial system which requires covering the largest range of transactions that pose money laundering and terrorist financing risks. Financial exclusion risks arise when persons have to seek their financial services from informal providers in the cash economy. These risks include financial crimes committed by informal service providers, as well as threats to the integrity of formal financial services, as due diligence inquiries fail when money trails disappear in the cash economy. Thus, ensuring that low income, rural sector or undocumented groups have access to regulated financial services helps to strengthen the implementation of AML/CFT measures. Within this spirit, FATF published in June 2011 a Guidance paper which provided support to countries and their financial institutions in designing AML/CFT measures that meet the national goal of financial inclusion. Following the revision of its Recommendations in February 2012, FATF adopted an updated version of its Guidance on financial inclusion in February 2013. This project was conducted in partnership with the World Bank and the Asia/Pacific Group on Money Laundering (APG), and in consultation with the financial industry. The purpose of the Guidance paper is to ensure that AML/CFT controls do not inhibit access to well regulated financial services for financially excluded and underserved groups. The document provides clarity and guidance on the FATF Recommendations that are relevant when promoting financial inclusion and shows how the Recommendations can be read and interpreted to support financial access. The

Guidance reviews the different steps of the AML/CFT process (Customer Due Diligence, record-keeping requirements, reporting of suspicious transactions, use of agents, internal controls), and for each of them presents how the Standards can be read and interpreted to support financial inclusion.

7. FINANCING PROLIFERATION

The FATF mandate was extended in 2008 to include new and emerging threats such as proliferation financing, which means financing the proliferation of weapons of mass destruction. In 2010, the FATF issued a document on financing proliferation entitled "Combatting Proliferation Financing: A Status Report on Policy Development and Consultation, 2010". It is a status report on the policy work and consultation being undertaken to that date in relation to proliferation financing. It develops an understanding of the issues surrounding proliferation financing and provides information that can be used by the FATF to assess the need for policy measures to counter it and to strengthen safeguards against it. In addition, the report outlines a series of options that could be considered by the FATF, and by countries, within the framework of existing United Nations Security Council Resolution 1540 of 2004.

The title of the FATF 40 new recommendations of February 2012 has changed to include in addition to the combatting of money laundering, the financing of terrorism and proliferation. In the body of the recommendations, recommendation 7 requires "countries to implement targeted financial sanctions to comply with the United Nations Security Council Resolutions (UNSCRs) relating to the prevention, suppression and disruption of proliferation of weapons of mass destructions (WMD) and its financing". These resolutions include resolution 1718 and 1737 of 2006, 1747 of 2007, 1803 of 2008, and 1929 of 2010 (see Recommendation 7, FATF 2012 a). The first resolution relates to the Democratic People's Republic of Korea while the remaining four address the case of the Islamic Republic of Iran. FATF had previously issued three guidance papers on the subject matter (see FATF 2013 a):

1. *The Implementation of Financial Provisions of UNSCRs to Counter the Proliferation of WMD* (June 2007)
2. *The Implementation of Activity-Based Financial Prohibitions of UNSCR 1737* (October 2007)
3. *The Implementation of Financial Provisions of UNSCR 1803* (October 2008)

The FATF's efforts in this area are consistent with the needs identified by the relevant UN Security Council Resolutions (UNSCRs). In recent years, the FATF has published

guidance to assist jurisdictions in their implementation of these resolutions. FATF also published a Typologies report which identified the issues surrounding proliferation financing and highlighted issues for further consideration. The new guidance of 2013 entitled "FATF Guidance: The Implementation of Financial Provisions of United Nations Security Council Resolution to Counter the Proliferation of Weapons of Mass Destruction" assists countries in implementing in addition to the targeted financial sanctions, other measures such as activity-based financial prohibitions and vigilance measures.

As far as banks are concerned, according to the new guidance, a number of additional issues arise where a bank or other financial institution is designated for the purpose of financial sanctions. In this respect, competent authorities should seek to implement financial sanctions as quickly as possible. In so doing, they should take a number of immediate actions: First, regulators should determine whether the designated bank has a presence in their country. Second, the authorities should also determine whether the designated bank has accounts in a bank located in its territory. Third, regulators should consider whether the designation of the bank will cause concerns relating to the bank's senior management, and consider whether the designation of the bank will cause other regulatory concerns, such as systemic risks (e.g. other banks suffering an adverse effect) or other market impacts (e.g. a run of creditors on the bank or potential disturbances in the payment systems). Such a determination may lead authorities to consider the appointment of an administrator or auditor, or other appropriate action. Fourth, the guidance discusses other issues related to payments made by the designated banks and payments due to the bank and whether they are due under prior contracts or are extraordinary payments. Fifth, the guidance document discusses cross-jurisdictional cooperation where countries containing branches or subsidiaries of a designated bank should communicate with each other to ensure that sanctions are being applied in a consistent and effective manner across countries.

8. GOVERNANCE/CORPORATE RESPONSIBILITY/ETHICS

The Basel Committee on Banking Supervision published initial guidance on corporate governance in 1999, with revised principles in 2006 aiming at assisting banking supervisors in promoting sound corporate governance practices. In October 2010, The Committee published the final document of "Principles for Enhancing Corporate Governance". Poor corporate governance is believed to contribute to bank failures with the possibility of broader macroeconomic implications, such as contagion risk and impact on payment systems. In addition, poor corporate governance could in turn trigger a bank run or liquidity crisis. Thus, from the perspective of the banking sector, corporate

governance involves the allocation of authority and responsibilities, including setting the bank's strategy and objectives, determining its tolerance for risk, protecting the interests of depositors, meeting shareholders' obligations, and taking into account the interests of other recognized stakeholders.

Drawing on the lessons learned during the latest financial crisis, the Committee in the document, "Principles for enhancing corporate governance", sets out best practices for banks in light of the crisis. The key areas where the principles have been strengthened include the role, qualifications and composition of the board, the importance of an independent risk management function monitoring risks, the board's oversight of the compensation systems and its understanding along with the bank's senior management of the bank's operational structure and risks, and the importance of supervisors regularly evaluating the bank's corporate governance policies and practices in line with the Committee's principles.

The Lebanese Central Bank in line with the Basel decisions amended basic decision 9382 of July 26, 2006 to come-up with intermediate decision 10708 of April 21, 2011 concerning "Corporate Governance". The new decision stated the following: "All banks operating in Lebanon must: 1- Spare no effort to comply with the principles issued and to be issued by the International Basel Committee for Enhancing Corporate Governance in Banking Institutions; and 2- Prepare their own "Corporate Governance Guide" that includes the following information at least: an administrative organizational chart, an organizational chart showing the relation between the parent bank and its subsidiaries or sister companies, the approach adopted by the bank to implement Corporate Governance principles, the Board of Directors' size, role, responsibility and composition (number of independent, executive and non-executive members), the criteria adopted to compute the compensation of the Board of Directors and Senior Management's members, the nature and work charter of each of the Board committees, the communication mechanism between the Board of Directors and the Senior Management, the rules adopted to assess the performance of the Senior Management and the Board of Directors regarding their compliance with Good Governance procedures, the Succession Plan to be adopted for selecting the Board of Directors and Senior Management's members, a summary of the Code of Conduct, the disclosure policy adopted, notably for preparing financial statements and addressing any conflict of interest, the possibility of granting the employee stock options for free, to enable him/her to buy stocks in the bank, if any, the method followed by the parent bank when dealing with affiliated banks and institutions".

The Basel document also emphasizes the corporate responsibility, values, and the code of conduct and ethics that need to be present in financial institutions. Thus, professional and responsible behavior is essential for proper governance. The board should take the lead in

establishing and setting professional standards and corporate values that promote integrity for itself, senior management and other employees. A bank's code of conduct, should articulate acceptable behavior by discouraging the taking of excessive risks and by preventing the bank from engaging in any improper or illegal activity, such as financial misreporting, money laundering, corruption fraud and bribery. The board should ensure that appropriate steps are taken to communicate throughout the bank the corporate values, professional standards or codes of conduct, together with supporting policies and procedures. An example of a policy largely relevant to board members is a conflict of interest one as conflicts of interest may arise as a result of the various activities and roles of the bank. The board should have a formal written conflicts of interest policy and an objective compliance process for implementing the policy.

According to the document, boards in many jurisdictions ought to establish certain specialized board committees with the number and nature of committees depending on the size of the bank and its board, the nature of the business areas of the bank, and its risk profile. For large and internationally active banks, an audit committee or equivalent should be required as well as a risk management committee or equivalent, responsible for advising the board on the bank's overall current and future risk tolerance and strategy, including strategies for capital and liquidity management, as well as for credit, market, operational, compliance, reputational and other risks of the bank. Based on this document, the Central Bank of Lebanon introduced Intermediate Decision No 10706 of April 21, 2011, amending Basic Decision No 9956 of July 21, 2008. The new decision stipulates in articles 4 and 7 that each bank should establish and audit committee and a risk committee.

A major area of interest in governance of financial institutions is the risk management and internal controls. The document recommends banks to have a risk management function that identifies, assesses, measures and monitors the key risks to the bank and to determine whether risk decisions are in line with the board-approved risk tolerance/appetite and risk policy while reporting to senior management, and the board as appropriate, on such issues. Internal controls are designed to ensure that each key risk has a policy, process or other measure to ensure process integrity, compliance and effectiveness. Internal controls also place checks on managerial and employee discretion. It is recommended that even in very small banks, for example, key management decisions should be made by more than one person ("four eyes principle"). Internal control reviews should also determine the extent of an institution's compliance with company policies and procedures, as well as with legal and regulatory policies. Finally, in line with corporate responsibility and proper ethical behavior, the governance of the bank should be adequately transparent to its shareholders, depositors, other relevant stakeholders and market participants.

9. HUMAN TRAFICKING/SMUGGLING OF MIGRANTS

The United Nations Convention against Transnational Organized Crime (UNTOC) which was developed by the United Nations Office on Drugs and Crime (UNODC) adopted by General Assembly resolution 55/25 of 15 November 2000, and entering into force on 29 September 2003 is the main international instrument in the fight against transnational organized crime. The Convention is supplemented by three Protocols, which target specific areas and manifestations of organized crime: the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children; the Protocol against the Smuggling of Migrants by Land, Sea and Air; and the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition. Countries must become parties to the Convention itself before they can become parties to any of the Protocols.

The Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children, was adopted by General Assembly resolution 55/25 to enter into force on 25 December 2003. It is the first international legally binding document with an agreed definition on trafficking in human beings to facilitate convergence in national approaches that would support efficient international cooperation in investigating and prosecuting cases of trafficking in humans. The Protocol also serves to protect and assist the victims of human trafficking. The Protocol against the Smuggling of Migrants by Land, Sea and Air, adopted by General Assembly resolution 55/25, entered into force on 28 January 2004. A major achievement was that a definition of smuggling of migrants was agreed upon for the first time in a Protocol that aims at preventing and combating the smuggling of migrants, as well as promoting cooperation among Member States, while protecting the rights of smuggled migrants. Issues on these two criminal activities remain some of the main concerns of UNODC as it organizes a major conference on Trafficking in Persons in Vienna on 6-8 November 2013 and one on smuggling of migrants on 11-13 November 2013.

According to UNODC, Trafficking in persons and smuggling of migrants are two concepts easily confused as they have many similarities. However, differences arise in three main issues related to consent, exploitation and trans-nationality. The smuggling of migrants involves migrants who have consented to the smuggling. Trafficking victims have either never consented or, if they initially consented, that consent has been rendered meaningless by the coercive, deceptive or abusive actions of the traffickers. Regarding exploitation, smuggling ends with the arrival of the migrants at their destination, whereas trafficking involves the ongoing exploitation to generate illicit profits for the traffickers. Smuggling is always transnational, whereas trafficking need not be. Trafficking can

occur regardless of whether victims are taken to another country or only moved from one place to another within the same country.

It is documented that even after the passage of the two conventions, criminals are increasingly turning to the trafficking of human beings and the smuggling of migrants given the high profitability of these illegal activities. The money generated by such activities finds its way into the financial system. As a result, FATF developed a report entitled "Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants" in July 2011 in which it addressed these two issues in major detail. The key objectives of the report are to assess the scale of the problem, identify different trends in these two criminal activities, determine from case studies the form that money laundering is taking and inform relevant law enforcement bodies and financial institutions of the results to assist in the suspicious transaction reports, and to increase the possibility of identifying and confiscating the proceeds of these criminal activities.

From the questionnaires and the case studies developed and addressed in the report, geographical differences related to the money laundering processes used exist as follows: In European countries, the traffickers/smugglers have great use of cash- intensive and money service businesses, cash couriers, hawala systems, front companies, and investments in high value goods such as cars and real estate; In American countries, there is a great use of casinos, import/export companies, cash-intensive (such as car dealership) and money service businesses, wire transfers, and online payments; In Asian countries, there is considerable commingling of funds with legitimate business proceeds and funds are more likely to be transferred via formal and informal banking systems; In African countries, there is likely to be purchase of real estate, investment in clubs or restaurants, offshore investments, informal banking systems, and use of agents/runners to carry cash.

Red flag indicators to assist financial institutions in their identification of money laundering from human trafficking/smuggling are reported as follows according to the report's major findings. For Banks, the usage of a common mobile number, address and employment references to open multiple accounts in different names; frequent money transfer to "risk" countries with concentration of "risk" nationalities among the opening of accounts; money rapidly withdrawn from accounts, from one ATM, or several ATMs in close proximity; frequent deposits or withdrawals with no apparent business source; third party cash deposits are made at various bank branches and via ATMs; transactions undertaken that appear inconsistent with customer profile; unusual withdrawals, deposits or wire activity inconsistent with normal business practices, or dramatic and unexplained change in account activity; numerous incoming money transfers or personal checks deposited into business accounts for no apparent legitimate purposes. For Money Service Businesses, small amounts sent to different recipients; small amounts sent with high

frequency to unconnected persons; frequent transfers to “risk” countries; multiple customers conducting international funds transfers to the same overseas beneficiary.

10. IDENTITY THEFT/ BENEFICIAL OWNERSHIP

Identity theft termed also as identity fraud refers to criminal behavior involving wrongfully using another person's personal data to usually achieve economic gain. Personal data especially identification cards, bank accounts, credit card and telephone numbers, home or work address, are some valuable information that can be used to achieve identity theft. Reports surface from many countries that unauthorized criminals have taken funds out of people’s bank or financial accounts, running up debts and committing financial crimes while using their names. In many cases, victims’ losses also include additional financial costs in trying to settle the crimes.

In the USA, The Department of Justice prosecutes cases of identity theft and fraud under a variety of federal statutes especially the “Identity Theft and Assumption Deterrence Act” passed by the Congress in 1998 (see Identity Theft and Assumption Deterrence Act). According to this department, statistics show that the average number of U.S. identity fraud victims annually amounts to 11,571,900, the percent of U.S. households that reported some type of identity fraud represents 7 %, the average financial loss per identity theft incident amounts to $4,930, the total financial loss attributed to identity theft in 2013 amounts to $21 billion rising from a figure of $ 13.2 billion in 2010. The type of fraud shows that the most common cases of identity theft are from the misuse of credit cards, followed by the misuse of bank accounts and thirdly from the misuse of personal information (see US Department of Justice).

Lately, Identity fraud has grown to include theft of cell and landline phone service; cable and satellite television service; power, water, gas and electric service; Internet payment service; medical insurance; home mortgages and rental housing; automobile, boat and other forms of financing and loans; and, government benefits.

The Huffington Post reports that one of the largest and most sophisticated identity theft cases ever seen in the U.S., according to Queens (N.Y.) District Attorney Richard Brown, involved a group of 111 people who were arrested for taking part in an operation that netted more than $ 13 millions between July and September 2011. The group would receive information about unknown people from various foreign countries, such as Russia and China, as well as via statewide suppliers — who would use a skimming device to swipe consumer credit card information at retail or food establishments — and illegal identification-gathering websites, according to the court documents. "Shoppers" would then be sent out on shopping sprees around the U.S. with counterfeit credit and I.D. cards

manufactured using the stolen information. Shoppers allegedly used the fraudulent cards to stay at five-star hotels, rent high-end cars, and even a private jet.

Beneficial ownership is enjoyed by anyone who has the benefits of ownership of an asset, and yet does not nominally own the asset itself. FATF recommendations 24 and 25 dealing with transparency and beneficial ownership of legal persons and arrangements state that countries should take measures to prevent the misuse of legal persons or arrangements for money laundering or terrorist financing. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons or trusts that can be obtained or accessed in a timely fashion by competent authorities.

11. MONEY REMMITANCE/CURRENCY EXCHANGE

Specialized financial businesses provide certain types of services, including money remittance (MR) and foreign currency exchange (CE). The service providers in this field (the "MR/CE sector") are quite diverse and range from simple to complex businesses. The MR/CE sector may provide significant opportunities for criminals aiming at laundering funds unless appropriate safeguards are in place. Particular risks involved with the sector are related not only to the misuse of MR/CE businesses for laundering money but also to the owning of such businesses by criminal groups and corrupt employees cooperating with criminals. Typologies reports published by the Financial Action Task Force (FATF) over the years have highlighted money laundering risks posed by bureaux de change (FATF typologies report, 1996, 1999 and 2001) and examined money laundering and terrorist financing vulnerabilities of alternative remittance systems (FATF typologies report 2004 -2005, see FATF 2010). The last report on the subject matter developed by FATF entitled "Money Laundering through Money Remmitance and Currency Exchange Providers (2010)" focuses on non-bank financial institutions that provide at least one of the following services: money remittance, currency exchange/dealing and issuing, cashing or redeeming of checks/money orders/stored value cards.

In most jurisdictions, MR/CE businesses are not defined as banks. National legislation has defined this group of financial service providers in some countries but not in most. In the United States, for example, the term money services business (MSBs) including non-bank financial institutions and MR/CE businesses has been defined since 1999. The duties of these businesses have also been defined in many countries after the FATF reports to prevent them as much as possible from money laundering and terrorist financing. In Lebanon for example, the Central Bank Intermediate circular number 337, decision number 11544, September 20, 2013, states in Article 1: "Exchange institutions

of Category A shall be the only institutions entitled to perform Hawala cash transfers, whether for their own account or on behalf of a third party. Therefore, while performing Hawala transactions, these institutions are prohibited from carrying out any of the banking transactions specified in the Code of Money and Credit, particularly from receiving deposits. Furthermore, pursuant to Law No 347 of August 6, 2001 on Regulating the Money Changer Profession in Lebanon, these institutions are also prohibited from performing transactions that do not fall within the scope of the exchange business, such as commercial financing, lending, and the management of funds, among others". Also in Article 5 of the same circular and decision, it was stated that "Any exchange institution that performs Hawala transactions must take all the procedures and measures needed to implement the obligations imposed by the applicable legal provisions, particularly the AML Law and all other regulations issued by Banque du Liban, the Banking Control Commission and the SIC (Special Investigation Commission). It must specifically comply with the requirements of Basic Decision No 11323 of January 12, 2013 relating to the Establishment of a Compliance Department, and adopt risk-based procedures and measures when checking the details of each incoming or outgoing Hawala transaction".

The FATF (2010) report examined how MR/CE businesses may be misused for money laundering purposes and identified vulnerabilities that may be exploited by criminals while viewing appropriate measures which could be taken to address the identified vulnerabilities. MR/CE providers can be used for money laundering in two ways: either by transactions without knowledge of the illegal origin or destination of the funds concerned or by a direct involvement of the service provider through complicity or takeover of such businesses by the criminal organization. Several features of the MR/CE sectors make them an attractive vehicle such as the cash character of transactions, their simplicity and certainty, their worldwide reach, the often less stringent customer identification rules that apply to such transactions compared with opening bank accounts, the reduced possibilities for verification of the customer's identification than in other financial institutions and the brevity of contacts with the service provider. Also important is that these transactions can be conducted in small denominations with relative ease through structuring or "smurfing" which appear to remain the most usual money laundering method of MR/CE providers and the most frequently reported suspicious activity. Structuring occurs when a person carries out several cash transactions in a single day or over a period of days through the same or several agents by breaking funds into smaller amounts in order to avoid the mandatory threshold reporting and/or customer identification requirements.

Available information gathered has allowed the money laundering threat facing MR/CE businesses to be documented. However, there was far less sector -specific information to work with regarding the threat of terrorist financing. The report then focused primarily on

the range of money laundering techniques to which MR/CE businesses may be vulnerable to providing a series of illustrative typologies. A non- exhaustive list of indicators of potentially suspicious activity related to the transactions or customers has been included in the report, to assist policy-makers.

12. ORGANIZED CRIME

Many of the topics discussed under various headings in this paper especially ones dealing with corruption, fraud, bribery, human trafficking, smuggling of migrants, identity theft, and cybercrime, can be considered as part of what is known as organized crime. According to the United Nations Office on Drugs and Crime (UNODC), organized crime threatens peace and human security, violates human rights and undermines economic, social, cultural, political and civil development of societies around the world.

Given that the domestic components of organized crime have been covered and discussed in several other sections, the foregoing analysis will focus on transnational organized crime that manifests itself in many forms, including trafficking in drugs, firearms and even persons, smuggling migrants and undermining financial systems through money laundering. Products that are illicit in nature are many times sourced from one jurisdiction or even continent, trafficked across another, and marketed in a third. Transnational organized criminals operate across borders as well as overcome cultural and linguistic differences.

The United Nations through UNODC developed and is currently the guardian of the United Nations Convention against Transnational Organized Crime (UNTOC) and the three Protocols -on Trafficking in Persons, Smuggling of Migrants and Trafficking of Firearms - that supplement it. UNTOC is the only international convention on organized crime representing the international community's commitment to combating transnational organized crime and acknowledging the UN's role in supporting this commitment. The development of the convention took place in Palermo, Italy, on 12-15 December 2000 (from here its name “Palermo Convention”) for signature by Member States at a High-level Political Conference convened for that purpose. Its adoption at the fifty-fifth session of the General Assembly of the United Nations in 2000 and its entry into force in 2003 reflects the commitment by the international community to counter organized crime. The Convention reflects the recognition by member jurisdictions and nations of the severity of organized crime, as well as the need to foster and enhance close international cooperation to tackle this criminal activity. By ratifying this convention states commit themselves to taking a series of measures against transnational organized crime, including the creation of domestic criminal offences (participation in an organized

criminal group, corruption, money laundering, and obstruction of justice); the adoption of frameworks for mutual legal assistance, extradition, and law enforcement cooperation; and the promotion of technical assistance and training programs for building or upgrading the necessary capacity of national authorities.

UNTOC does not precisely define the term transnational organized crime nor does it list the kinds of crimes included in it to allow for its applicability to new types of crime continuously emerging. However, the Convention defines organized criminal groups to include a group of three or more persons that was not randomly formed and has existed for a period of time. This group acts in concert with the aim of committing at least one crime punishable by at least four years' incarceration for the purpose of obtaining, directly or indirectly, a financial or other material benefit. UNTOC offers member nations and jurisdictions a framework for preventing and combating organized crime, and a platform for cooperating in doing so. As such, members of the Convention have committed to establishing the criminal offences of participating in an organized crime group, money laundering, corruption and obstruction of justice in their national legislation. Member states also have access to a new framework for mutual legal assistance and extradition, as well as a platform for strengthening law enforcement cooperation.

UNTOC deals with transnational crimes covering not only offences committed in more than one country or jurisdiction, but also those that take place in one State but are planned or controlled in another, crimes in one State committed by groups that operate in more than one State, and crimes committed in one State that have substantial effects in another State. The implied definition is thus broad encompassing serious criminal activities with international implications taking account global complexities and allowing cooperation on the widest possible range of common concerns.

The key feature of the UNTOC is its emphasis on international cooperation, especially in criminal matters. Thus, UNODC in addition to promoting and facilitating cooperation between different countries liaises between various nations and jurisdictions and international organizations and facilitates regional networks of cooperation against organized crime around the world. Specifically, UNODC is supporting the establishment and implementation of regional network of Central Authorities and of Prosecutors, such as the West African Network of Central Authorities and Prosecutors (WACAP) and the Network of Prosecutors against Organized Crime (REFCO).

The Protocol to Prevent, Suppress and Punish Trafficking in Persons, and the Protocol on the Smuggling of Migrants which supplemented the Palermo Convention have been addressed in section 9 of this paper. The Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition was adopted by

General Assembly resolution 55/255 of 31 May 2001and entered into force on 3 July 2005. The Protocol, which is the first legally binding instrument on small arms adopted at the international level, serves the objective to strengthen cooperation among Members in order to prevent and combat the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition. In signing the Protocol, Members make a commitment to adopt a series of crime-control measures and implement in their national laws several normative provisions to that effect.

13. PUBLIC PRIVATE COOPERATION/INTERNATIONAL COOPERATION/DATA SHARING

A major issue being addressed in the fight against financial and economic crimes is the cooperation among public, regulatory and private sectors, the international cooperation between various countries and jurisdictions and the data sharing among all groups concerned. FATF recommendation 2 entitled "National Cooperation and Coordination" states that countries should have national AML/CFT policies, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies. Countries should ensure that policy -makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policy -making and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

International cooperation is reflected in recommendation 36 which states that "countries should take immediate steps to become party to and implement fully the Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption (UNCAC), 2003; and the Terrorist Financing Convention, 1999. Where applicable, countries are also encouraged to ratify and implement other relevant international conventions, such as the Council of Europe Convention on Cybercrime, 2001; the Inter American Convention against Terrorism, 2002; and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005". As such, and in line with the Palermo convention on organized crime discussed in the relevant section, International cooperation against organized crime should be used as a tool for strengthening sovereignty and security. The United Nations Convention on Transnational Organized Crime (UNTOC) provisions on Mutual Legal Assistance (MLA), extradition, transfer of sentenced prisoners, and asset confiscation make it a practical tool in this area.

Different jurisdictions and countries can use the UNTOC to cooperate at both formal and informal levels. At the formal level, it can be used to request and deliver MLA, extradition, freezing and confiscation of criminal proceeds. The convention can also supplement bilateral and multilateral MLA and extradition agreements. Informal cooperation can take place between different authorities such as law enforcement, witness protection and financial intelligence ones to share criminal intelligence, cooperate in the protection of witnesses and share information concerning financial crimes respectively. UNODC continuously develops new tools to facilitate international cooperation, including manuals, an online directory of competent national authorities, a mutual legal assistance request writer tool, a legal database and best practices case law.

Additionally, MLA in recommendation 37 states that countries should provide mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions, and related proceedings. This is followed in recommendation 38 where countries should ensure that they have the authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered; Recommendation 39 relates to extradition requests where countries should constructively and effectively execute extradition requests in relation to money laundering and terrorist financing, without undue delay. In the case of asset recovery cases, countries require at least one of four legal bases to provide formal MLA. These legal bases are domestic legislation allowing for international cooperation in criminal cases, bilateral MLA agreements, promise of reciprocity through diplomatic channels and international conventions containing provisions on MLA in criminal matters.

14. TAX EVASION

The incentive to avoid and evade taxes has been prevalent in all societies due to the high tax burden in most countries. Thus, people may choose among four options: Tax compliance implying paying all taxes in full; tax avoidance which is legal in the sense that taxpayers deposit or invest their funds in tax shelters such as retirement accounts; tax evasion reflected in not reporting the return on investment or deposits to the home country to evade taxes which is illegal from the home perspective and legal in the haven itself. Evasion can also take place in any country by under-declaring income or over declaring deductions; and finally tax fraud where documents are falsified to hide the return which is fraudulent and illegal everywhere.

Several countries have historically acted as tax havens where banking and financial secrecy protect the identity of depositors and investors. The return on deposits or investments in these havens is either tax exempt or taxed at very low rates in comparison to the tax brackets in the country where the funds have originated. Thus, funds are

deposited in these havens without reporting their return to the country of the beneficiary. Lately, the US introduced the foreign account tax compliance act (FATCA) where countries are to sign an agreement with the USA through its internal revenue service to report bank interest income of US citizens to the US government preventing tax evasion. FATCA became law in the USA in March 2010. This law targets tax non-compliance by U.S. taxpayers with foreign accounts. It focuses on reporting by U.S. taxpayers about certain foreign financial accounts and offshore assets, and by foreign financial institutions about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest (see Foreign Account Tax Compliance ACT).

Several countries are currently in the process of introducing FATCA into their procedures. In Lebanon for example, the government approved and sent a law to the Lebanese parliament for approval regulating exchanging information related to tax evasion and fraud, giving Lebanon the legal basis to do so and to abide by OECD norms adopted by G20 countries. Lebanon will thus avoid sanctions imposed on countries lacking tax transparency and refusing to exchange tax information. The law incorporates strict procedures to prevent randomness and preserve at the same time stakeholders' rights (see Shahin, 2013).

Tax evasion has also been found in many smuggling and illicit activities. FATF developed in June 2012 a report entitled "The Illicit Trade in Tobacco (ITT)" in which it states that the revenues generated from ITT amount to an estimate of tens of billions of dollars. These revenues are hidden from tax authorities and may also be used to fund other forms of crime and terror. ITT therefore generates significant amounts of criminal proceeds, arising from both the trade itself and associated customs and tax offences.

15. WHISTLE BLOWING/REPORTING/WITNESS PROTECTION

There exist several concerns about disclosing information by public as well as private employees or agents when they suspect money laundering, financing terrorism or any criminal activity. The USA developed in 1989 "The Whistleblower Protection Act (WPA)" to protect public sector employees from retaliatory action for voluntarily disclosing information about dishonest or illegal activities occurring at a government organization. The law prohibits a federal agency from taking action, or threatening to take action, against these employees for disclosing such type of information (see Whistleblower Protection Act of 1989). In 2009 the Whistleblower Protection Enhancement Act (WPEA) was introduced to strengthen the legislation and became law in November 2012. The act provides millions of federal workers with the rights they

need to report government corruption and wrongdoing safely. The law reflects an unequivocal bipartisan consensus, having received the vote of every member in the 112th Congress, passing both the Senate and House of Representatives by unanimous consent shortly before adjournment (see Whistleblower Protection Enhancement Act).

FATF recommendation 20 deals with the reporting of suspicious transactions by stating that if a financial institution suspects that funds are the proceeds of a criminal or terrorist financing activity, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU) of its respective country or jurisdiction. Recommendation 21 on "Tipping-off and confidentiality" handles the witness protection issue by stating that the staff of financial institutions are to be protected by law from criminal and civil liability if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; However, this same staff are prohibited by law from disclosing ("tipping - off") the fact that a suspicious transaction is being filed with the FIU.

In the report of the Basel Committee on "Principles for Enhancing Corporate Governance" published in October 2010, under corporate values and code of conduct, it was stated that staff at all levels, with protection from any type of reprisal should be encouraged and able to communicate legitimate concerns about illegal, unethical or questionable practices. It is highly beneficial for banks to establish a policy on adequate procedures for employees to confidentially communicate their concerns. It becomes the duty of the board to determine how and by whom legitimate concerns shall be investigated and addressed, be it an internal control function, an objective external party, senior management, or even the board itself.

The Organized Crime Control Act of 1970 in the USA gave grand juries new powers, permitted detention of unmanageable witnesses, and gave the U.S. Attorney General authorization to protect witnesses, both state and federal, and their families. This last measure helped lead to the creation of WITSEC, an acronym for witness security (see Organized Crime Control Act). At more international levels, the United Nations Office on Drugs and Crime (UNODC) states that the cooperation of victims and witnesses is crucial to achieving successful prosecutions of criminal offenders. To help obtain such cooperation, and in accordance with Articles 24 and 25 of Organized Crime Convention, State parties shall take appropriate measures to provide effective protection to victims and witnesses of crime. Such measures may include establishing procedures to protect witnesses from threats, intimidation, corruption, or bodily injury and nations and jurisdictions are obliged to strengthen international cooperation in this regard.

CONCLUSION

There will always exist politically exposed persons aiming to build global retirement funds outside their jurisdictions and a corrupt component of the private sector seeking secret vehicles to launder its ill-gotten money. This demand-side for secrecy necessitates a supply-side for the secret market to develop, interact and flourish. Financial secrecy is fascinating in both its demand and supply components for actors coming-out of all segments of life in the pursuit of illicit gains. The variety of the financial and economic crimes addressed in this document represents major issues on both the demand and supply side of criminal activities with the very few non-covered topics falling largely into organized crime and corruption. However, the latest criminal activities addressed may not necessarily represent "new wine in old bottles". The criminal vehicles or the bottles are also changing necessitating dynamic policy responses requiring permanent updating, enhancement, implementation and coordination. According to UNODC, organized crime is not stagnant but adapts as new crimes emerge and as relationships between criminal networks become both more flexible and more sophisticated, with ever-greater reach around the globe. This underscores the dynamics of the dialectic stated and discussed in the introduction where regulators need innovation in the rules and market-place to remain abreast and capable of abating crime. On the performance front, these authorities have to a large extent succeeded in developing various conventions and rules to combat ill-gotten money especially inside domestic specific countries. The regulatory model has attempted to combat the supply side of secrecy as supply in this case motivates its own demand and curtailing it can contract financial crimes. Limiting the supply through various international and global coordinated measures is only the beginning as additional challenges remain in the enforcement and implementation. The evidence on the modest success of these measures is in the figures on asset recovery discussed in the relevant section showing that only minimal amounts were recovered from public and private sector corruption. Fighting a dynamic and evolving enemy gives a new meaning to "more is less" where more standard and deliberate reactions by regulators are lagging behind the adventurous profit motivated actions of the criminals and perpetrators. As Lewis Carroll, the author of "Alice's Adventures in Wonderland" interestingly stated in "Through the Looking-Glass" around 150 years ago, "It takes all the running you can do to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!"

REFERENCES

*Professor of Business Economics and Founding Dean (1996-2011), School of Business, Byblos, Lebanese American University.

Basel Committee on Banking Supervision (2010). "Principles for Enhancing Corporate Governance-Final Document", Bank for International Settlement, http://www.bis.org/publ/bcbs176.htm

Central Bank of Lebanon, Various Circulars and Laws, www.bdl.gov.lb

CNN (October 26, 2013). "Germany to send intelligence officials to Washington amid spying scandal" by Laura Smith-Spart and Per Nyberg, www.cnn.com.

Foreign Account Tax Compliance Act (FATCA 2010). http://www.irs.gov/Businesses/Corporations/Foreign-Account-Tax-Compliance-Act-(FATCA)

FATF (2013 a). "FATF Guidance: The Implementation of Financial Provisions of United Nations Security Council Resolution to Counter the Proliferation of Weapons of Mass Destruction", http://www.fatf-gafi.org/topics/financingofproliferation/

FATF (2013 b). "Revised Guidance on AML/CFT and Financial Inclusion", http://www.fatf-gafi.org/topics/financialinclusion

FATF (2013 c). "Best Practices Paper: The Use of the FATF Recommendations to Combat Corruption", http://www.fatf-gafi.org/topics/corruption/

FATF (2012 a). "International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation: the FATF Recommendations", http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

FATF (2012 b). "Illicit Tobacco Trade", http://www.fatf-gafi.org/topics/methodsandtrends/documents/illicittobaccotrade.html

FATF (2011). "Money Laundering Risks Arising from Trafficking of Human Beings and Smuggling of Migrants", http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneylaunderingrisksarisingfromtraffickingofhumanbeingsandsmugglingofmigrants.html

FATF (2010 a). "Money laundering through Money Remmitance and Currency Exchange Providers", http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneylaunderingthroughmoneyremittanceandcurrencyexchangeproviders.html

FATF (2010 b). "Combatting Proliferation Financing: A Status Report on Policy Development and Consultation", http://www.fatf-gafi.org/documents/documents/combattingproliferationfinancingastatusreportonpolicydevelopmentandconsultation.html

FATF (2008). "Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems", http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneylaunderingterroristfinancingvulnerabilitiesofcommercialwebsitesandinternetpaymentsystems.html

Identity Theft and Assumption Deterrence Act (1998), Public Law 105-318, 112 Stat. 3007 (Oct. 30, 1998), Congress of the USA, http://www.ftc.gov/os/statutes/itada/itadact.htm

International Symposium on Economic Crime (Thirty-First Symposium, 2103). "Fighting Economic Crime in the Modern World: the Role of the Private Sector-Partners and Problems", University of Cambridge, United Kingdom, www.crimesymposium.org.

International Symposium on Economic Crime (Thirtieth Symposium, 2012). "Economic Crime-Surviving the Fall, the Myths and Realities", University of Cambridge, United Kingdom, www.crimesymposium.org.

International Symposium on Economic Crime (Twenty-Ninth Symposium, 2011). "Responsibility for Risk", University of Cambridge, United Kingdom, www.crimesymposium.org.

Organized Crime Control Act of 1970 (Pub.L. 91–452, 84 Stat. 922 October 15, 1970), Congress of the USA.

Shahin, Wassim (2013). "Compliance with International Regulation on AML/CFT: the Case of Banks in Lebanon", *Journal of Money Laundering Control*, Volume 16, Number 2, pp. 109-118.

Stephenson K., Gray L., Power R., Brun J., Dunker G., and Panjer M., (2011). "Barriers to Asset Recovery ", Stolen Asset Recovery Initiative, The World Bank , UNODC.

The Huffington Post, 8/7/2012, "Largest Identity Theft Case in US History".

United Nations Office on Drugs and Crime (UNODC), Various Publications https://www.unodc.org/unodc/en/organized-crime/index.html, https://www.unodc.org/unodc/en/organized-crime/international-cooperation.html, https://www.unodc.org/unodc/en/organized-crime/technical-assistance.html

https://www.unodc.org/unodc/en/treaties/CTOC/CTOC-COP.html

http://www.unodc.org/unodc/treaties/CTOC/

U.S Department of Justice, Javelin Strategy and Research, 6-18-2013, "Identity Theft/Fraud Statistics".

US Treasury Financial Crime Enforcement Network (FinCEN), September 17, 2013, www.fincen.gov

Wall-Street Journal, September 27, 2013, "Cyber Warfare", Europe Edition, www.wsj.com.

Whistleblower Protection Act of 1989, Pub.L. 101-12, Congress of the USA

Whistleblower Protection Enhancement Act (2009, 2012) (WPEA) http://www.gpo.gov/fdsys/pkg/BILLS-112s743enr/pdf/BILLS-112s743enr.pdf