International Finance and Banking
ISSN 2374-2089
2017, Vol. 4, No. 2

Unintended Consequences of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)

George C. Georgiou

Towson University, University System of Maryland, Towson, Maryland, USA

E-mail: ggeorgiou@towson.edu

Received: June 9, 2017 Accepted: July 8, 2017 Published: August 10, 2017

doi:10.5296/ifb.v4i2.11375 URL: http://dx.doi.org/10.5296/ifb.v4i2.11375

Abstract

Money laundering is illegal world-wide and constitutes a significant economic inefficiency. One must wonder why current anti-money laundering and combating the financing (AML/CFT) efforts are primarily driven by the threat of terrorism and drug-trafficking when the overwhelming majority of illicit money flows is due to other causes, primarily fraud. The significant costs imposed on financial institutions, together with ever increasing levels of regulation mandated by AML/CFT efforts and the minuscule in comparison illicit money flows intercepted by these efforts has thereby resulted in both moral hazard and conflicts of interest for financial institutions. Furthermore, AML/CFT efforts take on a new meaning when one realizes that illicit money, flows not only through traditional banks but also shadow banks and other non-bank financial intermediaries. The costs of compliance are enormous in comparison to the benefits with the "war on terrorism" superseding the more relaxed "war on drugs", although even the latter was onerous in comparison to the even more relaxed efforts against the more widespread "white-collar" crime of fraud. In this paper, we trace the evolution of the present AML/CFT regime while at the same time assessing the costs and benefits of this government initiative on the efficiency of the financial system both in modern advanced economies and as well as the less developed economies of the world.

Keywords: Money laundering, Terrorism financing, Customer due diligence, Risk based Approach, Financial inclusion/exclusion, FATF blacklist, Offshore banks, Tax havens, Shadow banks, Eurocurrency, Digital currency, De-risking

1. Introduction

The common understanding of our modern market system, also known as "capitalism" or the "mixed economy" is quite removed from the classical understanding of the market system known as laissez-faire capitalism or "pure capitalism". Under the classical version of this system, the government's role is limited to protecting private property from theft and aggression and establishing a legal environment in which contracts would be enforced and citizens could interact in markets to buy and sell goods, services, and resources. In contrast, the modern market system is characterized by a mixture of centralized government economic initiatives and decentralized actions taken by individuals and firms. In this version of the market system as practiced by most countries, the government plays an active, but limited role in the economy. The necessity for this role for governments in modern advanced industrial economies is that although a laissez-faire market system promotes a high degree of efficiency in the use of its resources, it has certain inherent shortcomings, called "market failures" and/or "market distortions." (McConnell, 2015) Governments are thus charged with offsetting these "inefficiencies" and thus increasing the overall effectiveness of a market system. However, governments have their own set of shortcomings that can themselves cause substantial misallocations of resources. One such "government failure," or case of "government over-reach," depending on one's perspective, that has resulted in a misallocation of resources is typified in the government's Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) efforts. (FATF(12), Updated 2016)

While any effort on the part of the government to redress any inherent inefficiency or distortion of the laissez-faire market system is laudable, all such efforts have their costs and benefits. The aim of the present paper is to make the case that the costs to the financial system of these efforts, especially following the September 11, 2001 terrorist attacks in NYC and Washington, DC, and the ensuing emphasize on countering the financing of terrorism, have been substantially understated relative to the benefits. Part and parcel of this assessment is the complication resulting from the co-mingling of economic and political, i.e., national security, objectives and more specifically the "war on terrorism", which makes a purely economic analysis difficult to say the least. Matters are even further complicated when these efforts were widened to include violations of economic sanctions imposed on rogue regimes that are deemed to be "state sponsors of terrorism" or proliferators of weapons of mass destruction. Nonetheless, the global resources expended in this effort have been substantial both at the public and private level, yet there has been no evident reduction in illicit money flows worldwide even after the doubling off international efforts to combat these flows following the 9/11/2001 terrorist attacks. The argument that there has been no major organized terrorist attack on the U.S. homeland since 9/11 does not in-of-itself suffice to justify either the resource expenditures or the threat to individual privacy from these efforts. All the available data appears to indicate that the level of international terrorist financing is miniscule relative to illicit money flows due to fraud and drug trafficking that together represent well over 99% of the total money laundered globally.

Money laundering, of course, is illegal world-wide and constitutes a significant economic inefficiency. Per the United States Treasury Department, money laundering is the process of

making illegally-gained proceeds ("dirty money") appear legal ("clean"). (Treasury, 2015) Any reduction in illicit money flows is of course to be lauded and increases economic efficiency. Caught in the middle are the financial intermediaries "agents" that have been called upon to act on behalf of the government in its AML/CFT efforts. Many see this role as contrary to financial intermediaries' traditional role, under a laissez- faire system, of "honest broker" in the lender-borrower, or saver-investor, relationship. Financial intermediaries in this regard see themselves as "facilitators" in this relationship not "policemen." Others, while seeing their anti-money laundering role as necessary and consistent with their obligations as "good corporate citizens" in a mixed economic system, object to the high cost and increased level of scrutiny they are subject to in their day-to-day business activity. To put it simply, law-abiding citizens might be expected to take all necessary steps to secure their homes, e.g., install a home security system and report any suspicious activity in their neighborhoods, but they cannot be expected to replace the police by patrolling the neighborhood and apprehending wrong-doers.

Consequently, this presents a principal-agent problem in the bank-client relationship as has been made clear by the increasing number of money laundering cases brought against numerous financial institutions by law-enforcement agencies in recent years. The significant costs imposed on financial institutions, together with ever increasing levels of regulation mandated by AML/CFT efforts and the minuscule in comparison illicit money flows intercepted by these efforts has thereby resulted in both moral hazard and conflicts of interest for financial institutions. Recent cases of money laundering by some of the developed economies' largest and most sophisticated financial institutions, point to a systemic problem that goes beyond a simple breaking of the law by isolated individuals employed by these institutions. A small sample of money laundering cases includes

- In 2012, HSBC Holdings, a London-based company, paid nearly $2 billion in fines after it was discovered that the financial institution laundered money for drug traffickers, terrorists, and other organized crime groups throughout Iran. The laundering went on for many years before the activity was detected.

- In 2014, BNP Paribas, a French bank with global headquarters in London, pled guilty to falsifying business records after it was discovered the institution violated U.S. sanctions against Cuba, Sudan, and Iran. Thus, BNP was forced to pay a fine of $8.9 billion which is the largest fine ever imposed for violating those sanctions.

- In the 1980s, the Bank of Credit and Commerce International, a bank registered in Luxembourg and with offices in London, was found guilty of laundering an amount of money estimated to be in the billions for drug traffickers. (Legal Dictionary, 2017)

- In 2010, one of the biggest banks in America, Wachovia (now part of Wells Fargo), entered a Deferred Prosecution Agreement (DPA) (which has since expired) after the biggest ever action (estimated at $450 billion) was brought under the Bank Secrecy Act.

- In 2012, the British bank, Standard Chartered was accused, by New York's Department of Financial Services (DFS), of helping the Iranian government to circumvent US money laundering regulations to the tune of an estimated $287 billion over 10 years.

- In 1998, Russian criminals laundered an estimated $80 billion through shell banks in Nauru, an island northeast of Australia that had turned to offshore banking, leading to involvement in the "no questions asked" registration of offshore financial institutions. (Whitehead, 2017)

In this paper, we will attempt to trace the evolution of the present AML/CFT regime while at the same time assessing the costs and benefits of this government initiative on the efficiency of the financial system both in modern advanced economies and as well as emerging economies, including the less developed economies of the world.

2. US Anti-Money Laundering Efforts

Recent efforts by the U.S. to combat money laundering begin with the Bank Secrecy Act of 1970 (the BSA, or otherwise known as The Currency and Foreign Transactions Reporting Act of 1970) which requires financial institutions in the United States to assist U.S. government agencies to detect and prevent money laundering. The BSA requires businesses to keep records and file reports that are determined to have a high degree of usefulness in criminal, tax, and regulatory matters. The documents filed by businesses under the BSA requirements are heavily used by law enforcement agencies, both domestic and international to identify, detect and deter money laundering whether it is in furtherance of a criminal enterprise, terrorism, tax evasion or other unlawful activity. (IRS, 2016) More specifically, to mitigate the risks associated with the deposit or use of large sums of potentially illicit anonymous cash, the BSA established anti-money laundering customer identification, recordkeeping, and reporting obligations for financial institutions. Financial institutions are required to verify a customer's identity and retain records of certain information prior to issuing or selling bank checks and drafts, cashier's checks, money orders, and traveler's checks, when purchased with cash (bank notes) in amounts between $3,000 and $10,000. For cash transactions above $10,000, whether a single transaction or a series of related transactions with a customer in a single business day, financial institutions are required to file a Currency Transaction Report (CTR) with FinCen (Financial Crimes Enforcement Network). FinCen is a bureau of the United Stated Department of the Treasury that collects and analyzes information about financial transactions to combat domestic and international money laundering, terrorist financing, and other financial crimes. Other businesses must report cash transactions of more than $10,000 to the IRS (Internal Revenue Service) and FinCen. (Currency, 2016)

Money laundering is the conversion of "dirty" money into "clean" money whereby "dirty" money is money that has been derived by illegal means. Money laundering is a necessary consequence of almost all profit generating crimes and can occur almost anywhere in the world. It is difficult to estimate with any accuracy how much money is laundered in the US, however, per the latest US Treasury's National Money Laundering Risk Assessment (Treasury, 2015), about $300 billion is generated annually in illicit proceeds with fraud and drug trafficking offenses generating almost all those proceeds. The United Nations Office on

Drugs and Crime (UNODC) provides a similar estimate of $300 billion in illicit money flows from fraud and drug trafficking in the U.S. (Crime, 2011)

Fraud encompasses several distinct crimes, which together generate the largest volume of illicit proceeds in the US, roughly 80% of the total. Fraud perpetrated against federal government programs, including false claims for federal tax refunds, Medicare and Medicaid reimbursement, and food and nutrition subsidies; represent only one category of fraud but one that is estimated to generate at least twice the volume of illicit proceeds earned from drug trafficking. Healthcare fraud involves the submission of false claims for reimbursement, sometimes with the participation of medical professionals, support staff, and even patients. Federal government payments received illegally by check can be cashed through check cashing services, some of which have been found to be complicit in the fraud. Public corruption at the federal, state, local level, as well as foreign official corruption should also be noted. Use of the Internet to commit identity theft has expanded the scope and impact of financial fraud schemes. Personal identifying information and the information used for account access can be stolen through hacking or social exploits in which the victim is tricked into revealing data or providing access to a computer system in which the data is stored (Identity Theft). A stolen identity can be used to facilitate fraud and launder the proceeds. Stolen identity information can be used remotely to open a bank or brokerage account, register for a prepaid card, and apply for a credit card. (Treasury, 2015)

Drug trafficking, in contrast, is a cash business generating an estimated $64 billion annually from U.S. sales, or approximately 20 percent of the total illicit cash flows. Mexico is the primary source of supply for some drugs and a transit point for others. Although there are no reliable estimates of how much money Mexican drug trafficking organizations earn overall, estimates range from $6 billion to $39 billion. For cocaine, Mexican suppliers are estimated to earn about 14 cents of every dollar spent by retail buyers in the U.S. It is the thousands of low level drug dealers and distributors throughout the country who receive most of the drug proceeds. The severing by U.S. banks of customer relationships with Mexican money exchangers (casas de cambio) because of U.S. enforcement actions against U.S. banks between 2007 and 2013, combined with the U.S. currency deposit restrictions imposed by Mexico in 2010, are believed to have led to an increase in holding and using drug cash in the U.S. and abroad, because of placement challenges in both countries. This shifted some money laundering activity from Mexico to the U.S. (Treasury, 2015)

International organized crime groups, i.e., La Cosa Nostra (Mafia), African Criminal Enterprises, Eurasian Organized Crime, Middle Eastern Criminal Enterprises; target U.S. interests both domestically and abroad. The criminal activity associated with these groups includes alien smuggling, drug trafficking, extortion, financial fraud, illegal gambling, kidnapping, loan sharking, prostitution, racketeering, and money laundering. Some groups engage in white-collar crimes and co-mingle illegal activities with legitimate business ventures.

It is interesting to note that the Bank Secrecy Act of 1970 followed President Richard Nixon's 1969 formal declaration of a "war on drugs" that would be directed toward eradication,

interdiction, and incarceration. (Payan, 2013) This was followed in June 1971 with a special message from President Nixon to the Congress on Drug Abuse Prevention and Control—during which he declared drug abuse "public enemy number one". Today, the Drug Policy Alliance, which advocates for an end to the War on Drugs, estimates that the United States spends $51 billion annually on these initiatives. (Alliance, 2016) This is strikingly comparable to the $64 billion annually generated by drug trafficking estimated by the U.S. Treasury. This is not an attempt to present an argument for the general legalization of drugs but an indication of the difficulty in assessing the costs and benefits of combating money laundering, especially as it relates to the "war on drugs." It is also interesting to note that illicit money flows from drug trafficking in the U.S. represents no more than 20% of the total, yet was the driving force behind U.S. anti-money laundering efforts, from the passing of the Bank Secrecy Act of 1970 till the more recent passing of the USA Patriot Act of 2001 (formally known as Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) under President George W. Bush. The "war on drugs" has given way to the "war on terrorism" which has now become the new "public enemy number one".

Since the BSA was created, many other legislative acts and money laundering regulations have come about to strengthen the movement. These include:

- The Money Laundering Control Act of 1986, which prohibits engaging in any transactions involving proceeds generated from illegal activities.
- The 1988 Anti-Drug Abuse Act, which expanded the definition of "financial institution" to include car dealers and real estate personnel, requiring them to file reports on transactions involving large amounts of currency.
- The 1992 Annunzio-Wylie Anti-Money Laundering Act, which requires stricter sanctions for violations of the BSA, and requiring additional verifications, recordkeeping, and reporting for wire transfers.
- The Money Laundering Suppression Act of 1994 which requires banks to develop and institute training in anti-money laundering examination procedures.
- The Money Laundering and Financial Crimes Strategy Act of 1998 which requires banking agencies to develop training for examiners. (Legal Dictionary, 2017)

Unfortunately, as these money laundering regulations are put into place, criminals work to find new methods to prevent their activity from becoming detected or considered suspicious.

More recently, the USA Patriot Act of 2001 was passed in response to the September 11, 2001, terrorist attacks. The law is intended to help government agencies detect and prevent possible acts of terrorism, or sponsorship of terrorist groups. The law gave new powers to the U.S. Department of Justice, the National Security Agency and other federal agencies on domestic and international surveillance of electronic communications; it also removed legal barriers that had blocked law enforcement, intelligence and defense agencies from sharing information about potential terrorist threats and coordinating efforts to respond to them. The

Patriot Act raised concerns among civil liberties groups and other critics surrounding the data privacy rights of U.S. citizens, concerns that are beyond the scope of this paper. However, although the Patriot Act comprises 10 categories, called "titles", only one "title", Title III: Anti-Money Laundering to Prevent Terrorism, deals with money-laundering. (Management, 2016) In essence the USA Patriot Act is all about the "war on terrorism" but as a byproduct it has to a great extent hijacked anti-money laundering efforts that had already been sidetracked by the "war on drugs." Consequently, to the then existing Anti-Money Laundering efforts (AML), politically driven by the "war on drugs", was added the Combating the Financing of Terrorism (CFT), politically driven by the "war on terrorism", in what is now a symbiotic AML/CFT effort in which the number one objective, is combating terrorism, followed by drug trafficking. On the other hand, fraud, human smuggling, organized crime, and public corruption that represents up to 80% of illicit money flows is a distant third objective.

3. Money Laundering: "White-collar Crime"

One must wonder why current AML/CFT efforts are primarily driven by the threat of terrorism and drug-trafficking when the overwhelming majority of illicit money flows is due to other causes, primarily fraud. One possibility is the perception that money-laundering is a "white-collar crime" or possibly a "victimless crime". White-collar crime refers to financially motivated nonviolent crime committed by business and government professionals. Within criminology, it was first defined by sociologist Edwin Sutherland in 1939 as "a crime committed by a person of respectability and high social status in the course of his occupation". The term white-collar crime is now synonymous with the full range of frauds committed by business and government professionals. ...The motivation behind these crimes is financial—to obtain or avoid losing money, property, or services or to secure a personal or business advantage. (Investigation, 2016) White Collar crime can describe a wide variety of crimes, but they all typically involve crime committed through deceit and motivated by financial gain. The most common white collar crimes are various types of fraud, embezzlement, tax evasion and money laundering. Many types of scams and frauds fall into the bucket of white collar crime, including Ponzi schemes and securities fraud such as insider trading. More common crimes, like insurance fraud and tax evasion, also constitute white collar crimes. (FindLaw, 2016) The underlying premise of this perception of money laundering is that while it constitutes a crime, it is a "non-violent crime", and for the most part there are no victims other than the tax authorities. This might then explain the possible less than whole-hearted effort on the part of financial institutions and individuals within these institutions to take a forceful role in combating illicit money flows.

The process of money laundering per se is non-violent. It is defined as the conversion of "dirty" money into "clean" money. "Dirty" money is money that has been derived by illegal means. However, in several legal and regulatory systems, the term money laundering has become conflated with other forms of financial crime, and sometimes used more generally to include, misuse of the financial system (involving things such as securities, digital currencies, credit cards, and traditional currency), including terrorism financing, and evasion of international sanctions. Most anti-money laundering laws openly conflate money laundering (which is concerned with source of funds) with terrorism financing (which is concerned with

destination of funds) when regulating the financial system. Money laundering typically involves three steps: placement, layering, and integration. First, the illegitimate funds are furtively introduced into the legitimate financial system. This is referred to as "placement" and occurs when the cash is converted into "book" money. Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. This is referred to as "layering" or covering the tracks. The aim here is to delete the past or the "illegitimate origins" of the money. Finally, the money is integrated into the financial system through additional transactions until the "dirty money" appears "clean." This then allows for the acquisition of additional wealth from the transactions of the illicit funds, and ultimately provides a way to spend the funds while avoiding suspicions. Money laundering is concerned with the "source of funds" and there is no implication that the source of these illicit money flows is either "non-violent" or "victimless". Furthermore, the further the money is removed from its "source", the more likely is the perception that money laundering is more about tax avoidance than tax evasion. (About Business Crime Solutions Inc., 2017)

4. Financial Action Task Force (FATF) and the Internationalization of Anti-Money Laundering Efforts

Very early on, US law enforcement authorities realized that the "war on drugs" and anti-money laundering efforts in general, could not be won by simply passing US laws but required an internationally coordinated effort. Some of the international instruments and standards governing AML and CFT include:

- The 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances,
- The 2000 Convention against Transnational Organized Crime,
- The 2003 United nations Convention against Corruption, and most importantly,
- The Recommendations of the 1989 Financial Action Task Force (FATF) on Money Laundering, (and subsequently, post September 11, 2001, combating the Financing of Terrorism.

All these international instruments were designed to enforce money laundering laws to stop narcotics trafficking, international organized crime, and corruption, and subsequently the financing of terrorism. In a sense, unilateralism (the preferred path for implementing national policy) gave way to multilateralism (the coordinated path for implementing national policy) when nations realized that this battle could not be won by "going it alone" against an enemy that was global.

Key to this international effort was the Financial Action Task Force (FATF), set up as an independent inter-governmental body to develop and promote policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendation are recognized as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard. FATF was founded in 1989 on the initiative of the G7 (USA, UK, France, Germany, Italy,

Japan, Canada) to develop policies to combat money laundering (AML). Consequently, the Task Force has always had to deal with the image of being a "rich nations club" concerned with a problem that had a higher priority in the developed world than it had in the developing world. In 2001 the purpose of FATF was expanded to combat the financing of terrorism (CFT). It monitors countries' progress in implementing the FATF Recommendations by "peer reviews" based on mutual evaluations of member countries. The FATF Secretariat is housed at the headquarters of the Organization for Economic Cooperation and Development (OECD) in Paris, further enhancing its image of being a "rich nations club." Most OECD members are high-income economies with a very high Human Development Index (HDI) and are regarded as developed countries by all international standards.

The Task Force was charged with studying money laundering trends, monitoring legislative, financial and law enforcement activities taken at the national and international level, reporting on compliance, and issuing recommendations and standards to combat money laundering. At the time of its creation, the organization had 16 members. In its first year, the FATF issued a report containing Forty Recommendations to more effectively fight money laundering. These standards were revised in 2003 to reflect evolving patterns and techniques in money laundering. The mandate of the organization was expanded to include terrorist financing following the September 11, 2001 terrorist attacks, and 9 Special Recommendations (SR) on terrorism financing were added. Together, the Forty Recommendations (AML) and the 9 Special Recommendations on Terrorism Financing (CFT) set the international standard for anti-money laundering measures and combating the financing of terrorism and terrorist acts. Both sets of FATF Recommendations are intended to be implemented at the national level through legislation and other legally binding measures.

These recommendations are now known as Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) and were last updated in 2012. The Recommendations require states, among other things, to: implement relevant international conventions, criminalize money laundering and enable authorities to confiscate the proceeds of money laundering, implement customer due diligence (e.g., identity verification), record keeping, and suspicious transaction reporting requirements for financial institutions and designated non-financial businesses and professions, establish a financial intelligence unity to receive and disseminate suspicious transaction reports, and cooperate internationally in investigating and prosecuting money laundering. (FATF, 2017)

5. FATF Blacklist "Name and Shame"

As of 2017 FATF consists of thirty-five member jurisdictions and two regional organizations, the European Commission and the Gulf Co-Operation Council. The FATF also works in close co-operation with several FATF-Style international Regional Bodies (FSRBs) involved in combating money laundering and terrorism financing that are considered Associate and/or Regional Members. Furthermore, there are twenty-five International Observer Organization Members including for example the International Monetary Fund (IMF), the United Nations (UN) with 6 expert groups, and the World bank (WB). In total over 180 jurisdictions around the world have committed to the FATF Recommendations through the global network of

FSRBs and FATF memberships. (FATF, 2017)

In 2000 FATF issued a list of "Non-Cooperative Countries or Territories" (NCCTs), commonly called the "FATF Blacklist". This was a list of 15 jurisdictions that, for one reason or another, FATF members believed were uncooperative with other jurisdictions in international efforts against money laundering (and later, terrorism financing). Typically, this lack of cooperation manifested itself as an unwillingness or inability (frequently, a legal inability) to provide foreign law enforcement officials with information relating to bank account and brokerage records, and customer identification and beneficial owner information relating to such bank and brokerage accounts, shell company, and other financial vehicles commonly used in money laundering.

There are presently no "Non-Cooperative Countries and Territories" in the context of the NCCT initiative. However, FATF issues "Updates", as countries on the High-risk and non-cooperative jurisdictions list have made significant improvements in standard and cooperation ("Progress Reports"). The FATF also issues updates to identify additional jurisdictions that pose money laundering/terrorist financing risks ("Pseudo Blacklist" or "Gray List"). The effect of the FATF Blacklist has been significant, and arguably has proven more important in international efforts against money laundering than has the FATF Recommendations. While, under international law, the FATF Blacklist carried with it no formal sanction a jurisdiction placed on the FATF Blacklist often found itself under intense financial pressure.

Presently in 2017 there are only two countries, North Korea and Iran, that are identified as jurisdictions that have strategic deficiencies that pose a risk to the international financial system. Jurisdictions subject to FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the ongoing and substantial money laundering and terrorist financing (ML/TF) risks emanating from these jurisdictions. Most recently in 2016 several countries including: Algeria, Angola, Myanmar (Burma), Panama, and Papua New Guinea, were removed from the list of jurisdictions with strategic AML/CFT deficiencies after having made sufficient progress in addressing the deficiencies or had committed to an action plan developed with FATF to address the deficiencies. (FATF, 2017)

6. Offshore Financial Centers and Institutions

The list of FATF jurisdictions including Associate, Regional, and International Observer Organization Members is an indication of the global nature of the money-laundering problem. Of interest in this discussion is a category of jurisdictions and institutions known as Offshore Financial Centers that are commonly associated with discussions of money laundering but for the most part are neither on any FATF official blacklist or "gray list" given that low tax systems are perfectly legal under international law. Offshore financial centers are usually small, low-tax jurisdictions specializing in providing corporate and commercial services to non-residents in the form of offshore companies and the investment of offshore funds. An Offshore bank is a financial institution located outside the country of residence of the depositor, typically an offshore financial center, i.e., a low tax jurisdiction (or tax haven) that

provides financial and legal advantages. (IMF, 2017)

Offshore banks are a subset of what are known as Eurobanks. A Eurobank is a financial institution anywhere in the world which accepts deposits or makes loans in any foreign currency (i.e., engages in international banking). This foreign currency is referred to as Eurocurrency. Eurocurrency is deposits in banks (Eurobanks) that are located outside the borders of the country that issue the currency the deposit is denominated in. For example, a deposit denominated in Australian Dollars held in a South Africa bank is a Eurocurrency deposit. Likewise, a deposit denominated in US Dollars held in a Brazilian bank is a Eurocurrency deposit, or more specifically or more clearly a Eurodollar deposit. Eurocurrency does not have to involve either the Euro currency or the Eurozone. The four main Eurocurrencies are the US Dollar, the Eurozone Euro, the British Pound and the Japanese Yen; the currencies of the major developed economies of the world. Today the Eurocurrency and Eurobond markets are active because they avoid, domestic interest rate regulations, reserve requirements, and other barriers to the free flow of capital. The money market in which Eurocurrency is borrowed and lent by banks is known as the Eurocurrency Market. This Eurocurrency Market is utilized by large firms and wealthy individuals who wish to circumvent regulatory requirements, tax laws, reserve requirements, interest rate caps, and other barriers to the free flow of capital, that are often present in domestic banking, particularly in the United States. (Greco, 2017)

Offshore banking has proliferated in recent years due to its many advantages, including: greater privacy/confidentiality (bank secrecy), low or no taxation (tax havens), less regulation (less scrutiny, attracts high risk investments), easy access to deposits (at least in terms of regulation), and protection against local political or financial instability (unstable regimes and weak legal systems). While the term “offshore bank” originates from the Channel Islands being “offshore” from the United Kingdom, and most offshore banks are located on island nations to this day, the term is used figuratively to refer to such banks regardless of location, and includes Swiss banks and those of other landlocked nations such as Luxembourg and Andorra. Given the historical background of offshore banking, it is often associated with the: underground economy, organized crime via tax evasion, and money laundering. However, legally speaking, offshore banking does not prevent assets from being subject to personal income tax on interest. As much as half the world’s capital flows through offshore centers. Offshore tax havens have 1.2% of the world’s population and hold 26% of the world’s wealth, including 31% of the net profits of United States multinationals. An estimated $20-20 trillion is hoarded away in offshore accounts. In terms of offshore banking centers and in terms of total deposits, the global market is dominated by two key jurisdictions: Switzerland and the Cayman Islands. It might also be noted that the “original” offshore centers, Jersey, Guernsey, and the Isle of Man, for example, are known for their well-regulated banking infrastructure, however, many others are less structured and less regulated.

Furthermore, offshore banking can provide access to politically and economically stable jurisdictions. This will be an advantage for residents in areas where there is risk of political turmoil, or who fear their assets may be frozen, seized or disappear. Offshore banking may also provide higher interest rates than the legal rate in the home country, possibly due to

lower overheads and or a lack of government intervention. In addition, interest is generally paid by offshore banks without tax being deducted, and some offshore banks offer banking services that may not be available from domestic banks, such as, anonymous bank accounts, higher or lower rate loans based on risk, and investment opportunities not available elsewhere. Offshore banking is often linked to other structures, such as offshore companies, trusts or foundations, which may have specific tax advantages. Many advocates of offshore banking also assert that the creation of tax and banking competition is an advantage of the industry, arguing that tax competition allows people to choose an appropriate balance of services and taxes. Critics of the industry, however, claim this competition as a disadvantage, arguing that it encourages a "race to the bottom" in which governments in developed countries are pressured to deregulate their own banking systems to prevent the offshoring of capital.

Safe to say, the critics of offshore banking enumerate just as many disadvantages. They would argue that offshore bank accounts are sometimes less financially secure, and that offshore banking has been associated in the past with the underground economy and organized crime through money laundering. Following September 11, 2001, offshore banks and tax havens, along with clearing houses, have been accused of helping various organized crime gangs, terrorist groups, and other state or non-state actors. Offshore jurisdictions are often remote, and therefore costly to visit, so physical access and access to information can be difficult. Offshore private banking is usually more accessible to those on higher incomes, because of the costs of establishing and maintaining offshore accounts. As indicated earlier, the Bank Secrecy Act requires U.S. Taxpayers to file a Department of the Treasury Form 90-22.1 Report of Foreign bank and Financial Accounts (FBAR). However, when all is said and done, offshore banking is a legitimate financial exercise undertaken by many expatriate and international firms and workers, yet at the same time continues to arouse suspicion by its very nature and its historical associations. (Borrero & Errico, 2017)

7. Tax Havens and Bank Secrecy

A common association of offshore financial centers is "tax havens." A tax haven is a country or jurisdiction where certain taxes are levied at a low rate or not at all. Alternatively, it might be a country whose laws and other measures can be used to evade or avoid the tax laws or regulations of other jurisdictions. Or, simply a country which modifies its tax laws to attract foreign capital. Offshore banks operating in such tax havens can help effectively bypass complicated settlement processes and conduct SWIFT transactions with customers in overseas accounts. SWIFT (The Society for Worldwide Interbank Financial Telecommunication) is based in Brussels and operates a worldwide financial messaging network which exchanges messages between banks and other financial institutions.

The U.S. following September 11, 2001, had a secret Terrorist Finance Tracking Program (TFTP) to access the SWIFT database, rendering offshore banking for privacy severely compromised. Despite protests from certain European quarters regarding this invasion of privacy, an international effort has been ongoing ever since to weaken bank secrecy. For example, since starting to survey offshore jurisdictions in 2009, the OECD has been at the forefront of a crackdown on tax evasion, and will not object to governments using stolen

bank data to track down tax cheats in offshore centers, such as in the 2008 Liechtenstein tax affair. Liechtenstein, was one of the remaining uncooperative tax havens, as identified by FATF on money laundering at the time along with Andorra and Monaco. The recent sharing of confidential UBS Bank (Switzerland) details about 285 clients suspected of willful tax evasion by the United States Internal Revenue Service (IRS)was ruled a violation of both Swiss law and the country's constitution by a Swiss federal administrative court. Nevertheless, OECD has removed 18 countries, including Switzerland, Liechtenstein and Luxembourg, from its so-called "Grey List" of nations that did not offer sufficient tax transparency, and has re-categorized them as "White List" nations. (Global Financial Integrity, 2017)

8. Shadow Banks and other Non-Bank Financial Intermediaries (NBFIs)

AML/CFT efforts take on a new meaning when one realizes that illicit money flows not only through traditional banks but also shadow banks and other non-bank financial intermediaries. A financial intermediary is an institution that facilitates the channeling of funds between lenders and borrowers. That is, savers (lenders) give funds to an intermediary institution (such as a bank), and that institution gives those funds to investors (borrowers). This may be in the form of loans or other forms of investments. The list of financial intermediaries includes: commercial banks, mutual savings banks, savings and loan associations, building societies, credit unions, financial advisers or brokers, insurance companies, collective investment schemes, and pension funds. (Kodres, 2017)

A non-bank financial institution (NBFI) or shadow bank is a financial institution that does not have a full banking license or is not supervised by a national or international banking regulatory agency. NBFIs facilitate bank-related financial services, such as investment, risk pooling, contractual savings, and market brokering. Examples of NBFIs include: insurance firms, pawn shops, cashier's check issuers, check cashing locations, payday lending, currency exchanges, and micro-loan organizations. (The World Bank, 2017)

To complicate matters one can add informal and underground money transfer systems, such as Hawala; and digital currency, such as Bitcoin, that is created and held electronically. Hawala (or Hewala, also known as Hundi) meaning "transfer", is an informal value transfer system based on the performance and honor of a huge network of money brokers, primarily located in the Middle East, North Africa, the Horn of Africa, and the Indian subcontinent, operating outside of, or parallel to, traditional banking, financial channels, and remittance systems. Hawala is believed to have arisen in the financing of long-distance trade around the emerging capital trade centers in the early medieval period. In South Asia, it appears to have developed into a fully-fledged money market instrument, which was only gradually replaced by the instruments of the formal banking system in the first half of the 20th century. Today, Hawala is probably used mostly for migrant worker's remittances to their countries of origin. In the hawala system, money is transferred via a network of hawala brokers, or "hawaladors." It is "money transfer without money movement." The unique feature of the system is that no promissory instruments are exchanged between the hawala brokers; the transaction takes place entirely on the honor system. As this system does not depend on the legal enforceability

of claims, it can operate even in the absence of a legal and judicial environment. Trust and extensive use of connections, such as family relations and regional affiliations, are the components that distinguish it from other remittance systems. (U.S. Department of the Treasury, 2017)

It is precisely this characteristic of any such informal money transfer system that presents a problem for any anti-money laundering efforts and even more so for any efforts to combat the financing of terrorism. All AMT/CFT efforts are based on the elimination of the "informal" financial system. Only if all financial transactions are part of the formal economy do AMT/CFT efforts have any chance of being successful. This is why AMT/CFT efforts necessitated a compromise with financial institutions to reduce the high-cost, comprehensive and intrusive efforts to monitor all financial transactions, and replace them with a "Risk Based" Approach, i.e., a focus on transactions and entities that represented a "red flag" based on a risk-based assessment; and in return authorities would join efforts with the financial institutions to bring into the formal banking system the substantial informal banking sector, i.e., "the un-banked segments of the world's population", especially in the emerging economies of the world that could prove a bonanza for the financial institutions over the long-term.

Informal money transfer systems such as hawala, are attractive to customers because they provide a fast and convenient transfer of funds, usually with a far lower commission than that charged by banks. Its advantages are most pronounced when the receiving country applies unprofitable exchange rate regulations (as has been the case for many typical receiving countries such as Egypt) or when the banking system in the receiving country is less complex (e.g., due to differences in legal environment in places such as Afghanistan, Yemen, and Somalia). A lax or non-existent legal system and often the lack of personal security due to war and terrorist activity in such places is compounded by efforts by Western nations to prevent the flow of funds to these nations, leaving individuals with family and business ties with no other alternative than to resort to these "hawala" forms of money transfers. Moreover, in some parts of the world it is the only option for legitimate fund transfers, and has even been used by aid organizations in areas where it is the best-functioning institution. (El-Qorchi, 2002)

While the transfer of purchasing power remains primarily through the medium of national currencies, there is the growing use of alternative systems such as Bitcoin. Bitcoin is a form of digital currency, created and held electronically. No one controls it, including financial institution, central bank, or national government. Bitcoins aren't printed, like Dollars or Euros, but instead are produced by people, and increasingly businesses, running computers all around the world, using software that solves mathematical problems. Thus, Bitcoins are mathematically generated as the computers in this network execute difficult number-crunching tasks, a procedure known as Bitcoin "mining". There is no way for a central bank or any other entity to issue a flood of new Bitcoins and devalue those already in circulation as the mathematics of the Bitcoin system were set up so that the total number that can ever be "mined" is limited to around 21 million. The entire network is used to monitor and verify both the creation of new Bitcoins through mining, and the transfer of Bitcoins

between users. Bitcoins can be bought and sold in exchange for traditional currency on several exchanges, and can be directly transferred anonymously from one user to another across the internet. This makes Bitcoin and similar virtual currencies, also known as cryptocurrencies, attractive currency in which to settle international transactions, bypassing both bank charges and exchange rates. It goes without saying that the anonymity of Bitcoins and the omission of both bank transactions costs and exchange rates, make such a system quite appealing to activities such as money laundering or illegal drug dealings. While Bitcoins might not be the sole or only player in this area, it is certain that virtual currencies will have a future in the global financial system, once the software has been perfected, and the valuation of these virtual currencies has become less volatile, especially as virtual currencies are accepted and integrated into the traditional financial markets. They must, of course, first overcome the reluctance of sovereign issuers of traditional fiat currencies that have the most to lose from this potential rival. (The Economist, 2017)

9. Vulnerabilities and Risks

The vulnerabilities and risks of the existing financial system for illicit money transfers. i.e., money laundering, is inherently obvious to most observers. An understanding of any monetary system starts with cash or bank notes. The widespread use of cash, makes it difficult for authorities to differentiate between licit and illicit use and movement of bank notes. The use of cash and monetary instruments in amounts under regulatory recordkeeping and reporting thresholds will continue to be a problem. Cash, while necessary and omnipresent, is also an inherently fungible monetary instrument that carries no record of its source, owner, or legitimacy. Cash generated from drug trafficking or fraud can be held or spent as cash. Cash is an essential component of the U.S. and global economies, and of money laundering. There was approximately $1.36 trillion of U.S. banknotes in circulation as of March 11, 2015, and much of that currency circulates globally. But it is not just cash, it is also “near money” or “almost money” such as cashier’s checks, money orders, nonbank wire transfers, prepaid debit cards, and traveler’s checks that criminals can buy to use instead of cash for purchases or bank deposits. Transactions with cash and cash alternatives can be structured to stay under the recordkeeping and reporting thresholds, and case examples demonstrate that some merchants will accept more than $10,000 in cash without reporting the transaction as required. (U.S. Department of the Treasury, 2015)

While cash is the main medium for illicit money transfers, banks and other financial institutions are the conduits of these cash flows explicitly or implicitly. This might entail opening bank and brokerage accounts using nominees to disguise the identity of the individuals who control the accounts. To move funds into an account at a bank or broker-dealer, case examples show criminals may use an individual, serving as a nominee, to open the account and shield the identities of the criminals who own and control the funds. Alternatively, the account may be opened in the name of a business that was created to hide the beneficial owner who controls the funds. This then raises the issue of complicit violators within financial institutions. Of course, this is not the sole responsibility of financial institutions, given that the existing legal system enables the creation of legal entities without accurate information about the identity of the beneficial owner. In that regard, individuals and

entities can disguise the nature, purpose, ownership, and control of bank financial accounts.

Fraud of course is the main explanation for the misuse of products and services resulting from the deficient compliance with anti-money laundering obligations. Anti-money laundering compliance deficiencies are an inevitable consequence of a financial system with hundreds of thousands of locations for financial services. This is compounded by the millions of merchants that together with financial institutions wittingly facilitate illicit activity in what is known as trade based money laundering (TBML). TBML can involve various schemes that disguise criminal proceeds through trade-related financial transactions. One example of such schemes is the Black Market Peso Exchange (BMPE) which involves money brokers making local currency available in Latin America and Asia for drug dollars in the United States. Another form of TBML involves criminals using illicit proceeds to purchase trade goods, both to launder the cash and to generate additional profits. (U.S. Department of the Treasury, 2015)

10. Money Laundering Methods

There are two motives for laundering dirty money. First, is to avoid suspicion which necessitates the need to remove all traces that may indicate a crime was committed, i.e., the "dirty money" needs to "cleaned." Second, is to avoid detection which necessitates the need to shield the money from attempts to confiscate it. The amount of money laundered in the USA was estimated in the 2015 National Money Laundering Risk Assessment (NMLRA) of the US Treasury to be about $300 billion annually. The United Nations Office on Drugs and Crime (UNODC) provides a similar estimate of $300 billion annually. As indicated above, fraud and drug trafficking offenses generate most of those proceeds. UNODC estimates illicit drug sales were $64 billion (20%), putting the proceeds for all other forms of financial crime in the United States at $236 billion (80%), most of which is attributable to fraud.

Of course, the amount of money laundered world-wide is much higher. Criminals, especially drug traffickers, may have laundered around $1.6 trillion, or 2.7 per cent of global GDP, in 2009, per a report by UNODC. This figure is consistent with the 2 to 5 per cent range previously established by the International Monetary Fund (IMF) to estimate the scale of money-laundering. Regardless of the difficulty in measurement, the amount of money laundered each year is in the billions (US Dollars) and poses a significant policy concern for all governments. Thus, governments and international bodies have undertaken efforts to deter, prevent, and apprehend money launderers. Financial institutions have likewise undertaken efforts to prevent and detect transactions involving dirty money, both because of government requirements and to avoid the reputational risk involved.

Compounding the difficulty of enforcing anti-money laundering laws are the multitude of money laundering methods, including: structuring, bulk cash smuggling, cash-intensive businesses, trade-based laundering, shell companies and trusts, round-tripping, bank capture, casinos, real estate, and black salaries, just to name the most obvious. "Structuring," often known as smurfing, is a method of placement whereby cash is broken into smaller deposits of money, used to defeat suspicion of money laundering and to avoid anti-money laundering reporting requirements. A sub-component of this is to use smaller amounts of cash to

purchase bearer instruments, such as money orders, and then ultimately deposit those, again in small amounts.

"Bulk cash smuggling" involves physically smuggling cash in large amounts, usually greater than $10,000, to another jurisdiction and depositing it in a financial institution, such as an offshore bank, with greater bank secrecy or less rigorous money laundering enforcement. In the case of "cash-intensive businesses," a business typically expected to receive a large proportion of its revenue as cash uses its accounts to deposit criminally derived cash. Examples include: parking buildings, strip clubs, tanning beds, car washes, and casinos. Per the Federal Reserve, of the U.S. currency in circulation, approximately three-quarters is in the form of $100 bank notes, and about three-quarters of those U.S. $100 bills are held outside the United States.

"Trade-based laundering" involves under-or overvaluing invoices to disguise the movement of money. Furthermore, trusts and shell companies can disguise the true owner of money. Trusts and corporate vehicles, depending on the jurisdiction, need not disclose their true, beneficial, owner. In the case of "round-tripping," money is deposited in a controlled foreign corporation offshore, preferably in a tax haven where minimal records are kept, and then shipped back as a foreign direct investment, exempt from taxation. Another money laundering method is "bank capture." In this case, money launderers or criminals buy a controlling interest in a bank, preferably in a jurisdiction with weak money laundering controls, and then move money through the bank without scrutiny.

"Casinos" and "real estate" are also often the focus of money laundering methods. In the case of casinos, an individual may walk into a casino and buys chips with illicit cash. The individual will then play for a relatively short time. When the person cashes in the chips, they will expect to take payment with a check, or at least get a receipt so they can claim the proceeds as gambling winnings. With real estate, someone purchases real estate with illegal proceeds and then sells the property. To outsiders, the proceeds from the sale look like legitimate income. Alternatively, the price of the property is manipulated; the seller agrees to a contract that under-represents the value of the property, and receives criminal proceeds to make up the difference.

Lastly, In the case of "black salaries," a company may have unregistered employees without a written contract and pay them cash salaries. Dirty money might be used to pay them. Ultimately, the goal of money laundering is to be able to use the dirty money for private consumption. If unable to use it openly, the traditional way to keep the dirty money near is hiding it as cash at home or other places. A more modern method is a credit card connected to a tax haven bank. (Financial Action Task Force, 2005)

11. Enforcement and the Role of Financial Institutions

Anti-money laundering (AML) is a term mainly used in the financial and legal industries to describe the legal controls that require financial institutions and other regulated entities to prevent, detect, and report money laundering activities. As indicated previously, anti-money laundering guidelines came into prominence globally because of the formation of the

Financial Action Task Force (FATF) and the promulgation of an international framework of anti-money laundering standards. These standards began to have more relevance following the terrorist attacks of September 11, 2001, after FATF began a process to publicly identify countries that were deficient in their anti-money laundering laws and international cooperation, a process colloquially known as "name and shame", i.e., the FATF "Blacklist." This process took on greater urgency as combating the financing of terrorism gathered momentum to the point that many observers and jurisdictions view it as the driving force behind the present anti-money laundering efforts. (Financial Crimes Enforcement Network, 2017)

An effective AML program requires a jurisdiction to have criminalized money laundering; have given the relevant regulators and police the powers and tools to investigate; can share information with other countries as appropriate; and require financial institutions to: identify their customers, establish risk-based controls, keep record, and report suspicious activities. In terms of criminalizing money laundering, the elements of the crime of money laundering are set forth in the United Nations Convention Against Illicit Traffic in Narcotic Drugs (1988), the Convention Against Transnational Organized Crime (2000), and the Convention Against Corruption (2003). It is defined as knowingly engaging in a financial transaction with the proceeds of a crime for concealing or disguising the illicit origin of the property from governments. While banks operating in the same country generally must follow the same AML laws and regulations, financial institutions all structure their AML efforts slightly differently. Today, most financial institutions operating globally, and many non-financial institutions, are required to identify and report transactions of a suspicious nature to the financial intelligence unit in their respective country.

Under AML laws and regulations, all financial institutions are required to "identify customers." For example, a bank must verify a customer's identity and, if necessary, monitor transactions for suspicious activity. This is often termed as "know your customer" (KYC). This means knowing the identity of the customer and understanding the kinds of transactions in which the customer is likely to engage. In addition, financial institutions are required to "identify and report anomalies." By knowing one's customers, financial institutions can often identify unusual or suspicious behavior, termed anomalies, which may be an indication of money laundering. Bank employees, such as tellers and customer account representatives, are trained in anti-money laundering and are instructed to report activities that they deem suspicious. Additionally, anti-money laundering software filters customer data, classifies it per level of suspicion, and inspects it for anomalies. Such anomalies include any sudden and substantial increase in funds, a large withdrawal, or moving money to a bank secrecy jurisdiction.

Smaller transactions that meet certain criteria may also be flagged as suspicious. For example, structuring can lead to flagged transactions. The software also flags names on government "blacklists" and transactions that involve countries hostile to the host nation. Once the software has mined data and flagged suspect transactions, it alerts bank management, who must then determine whether to file a report with the government. (Sullivan & Cromwell LLP, 2016)

12. A Risk Based Approach (RBA) to AML/CFT

An evaluation of the costs and benefits of the AML enforcement outlined above plus the associated privacy concerns this raised has resulted in what is now termed the "risk based approach" (RBA) to AML/CFT. Leading the charge was the financial services industry which has become more vocal about the rising costs of anti-money laundering regulation and the limited benefits that they claim it brings. On the other hand, government-linked economists have noted the significant negative effects of money laundering on economic development, including undermining domestic capital formation, depressing growth, and diverting capital away from development.

Besides economic costs to implement anti-money-laundering laws, improper attention to data-protection practices may entail disproportionate costs to individual privacy rights. Groups in the EU and the USA such as the American Civil Liberties Union (ACLU) have expressed concern that money laundering rules require banks to report on their own customers, essentially conscripting private businesses "into agents of the surveillance state."

Rather than a blanket surveillance of all financial transactions, the risk-based approach (RBA) argues that once money laundering and terrorist financing (ML/TF) risks are properly understood, country authorities may apply AML/CFT measures in way that ensures they are commensurate with those risks. The objective of the RBA is to ensure AML/CFT measures are commensurate with the "risks identified," as well as to enable decision making on effective resource allocation. Risk assessments carried out by countries should be used for determining higher and lower risks that may then be addressed by applying enhanced measures or allowing simplified measures respectively. Financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs) should also be able to identify, assess and take effective action to mitigate ML/TF risks. Countries should then take steps to identify and assess their ML/TF risks on an "ongoing basis." (Financil Action Task Force, 2014)

13. Assessing Money Laundering and Terrorism Financing (ML/TF) Risk

Risk is a function of three factors: threat, vulnerability, and consequence. A threat is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. Vulnerabilities comprises those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk assessment context, looking at vulnerabilities as distinct from threat means focusing on, for example, the factors that represent weaknesses in AML/CFT systems or controls or certain features of a country. They may also include the features of a sector, a financial product or type of service that make them attractive for ML or TF purposes. Consequence refers to the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. The key is that the risk assessment adopts an approach that attempts to distinguish the extent of different risks to assist with prioritizing mitigation efforts.

ML/TF risk assessment comprises of three stages: identification, analysis, and evaluation. Identification starts by developing an initial list of potential risks or risk factors countries face

when combating ML/TF. Analysis lies at the heart of the ML/TF risk assessment process. It involves consideration of the nature, sources, likelihood and consequences of the identified risks or risk factors. Evaluation involves taking the risks analyzed during the previous stage to determine priorities for addressing them. (Financil Action Task Force, 2014)

14. Guidance for Banking

The risk-based approach (RBA) is central to the effective implementation of the revised FATF International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, which were adopted in 2012. The RBA means that countries, competent authorities and financial institutions, are expected to identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks to mitigate them effectively. In the case of banks, this applies to the way banks allocate their compliance resources, organize their internal controls and internal structures, and implement policies and procedures to deter and detect ML/TF.

Examples of ML/TF risk associated with different banking activities include retail banking, corporate and investment banking, investment services (or wealth management), and correspondent banking. Retail banking involves banks offering products and services directly to individual and business customers (including legal arrangements), such as checking accounts, loans (including mortgages) and savings products. This includes provision of services to cash-intensive business, volume of transactions, high-value transactions, and diversity of services. Corporate and investment banking involves banks providing corporate finance and corporate banking products and investment services to corporations, governments and institutions. This includes layering and integration, transfer of assets between parties in exchange for cash or other assets, and the global nature of markets. Investment services (or wealth management) involves banks providing products and services to manage their customers' wealth (sometimes referred to as private banking). This entails a culture of confidentiality, difficulty to identify beneficial owners, concealment (use of offshore trusts), banking secrecy, complexity of financial services and products, Politically Exposed Person (PEPs), high value transactions, and multiple jurisdictions. Correspondent banking involves high value transactions, limited information about the remitter and source of funds, especially when executing transactions with a bank located in a jurisdiction that does not comply or complies insufficiently with FATF Recommendations, and the possibility that PEPs are involved regarding the ownership of a bank. (Federal Financial Institutions Examination Council BSA/AML InfoBase, 2017)

15. Bank Risk Mitigation and Customer Due Diligence (CDD)

To mitigate bank risk, banks are expected to engage in Customer Due Diligence (CDD). CDD process are expected to be designed to help banks understand who their customers are by requiring banks to gather information on what their customers do and why they require banking services. Based on a holistic view of the information obtained in the context of their application of CDD measures, banks should be able to prepare a customer risk profile (CRP). This will determine the level and type of ongoing monitoring, and support the bank's decision whether to enter, continue or terminate, the business relationship. Risk profiles can apply at

the individual customer level or, where groups of customers display homogenous characteristics (for example, clients with similar income range, or conducting similar types of banking transactions) can be applied to such groups. This approach is particularly relevant for retail banking customers. (Basel Committee on Banking Supervision, 2014)

CDD comprises, first, identifying the customer and, where applicable, the customer's beneficial owner. Second, verifying the customer's identity based on reliable and independent information, data or documentation to at least the extent required by the applicable legal and regulatory framework. And, third, understanding the purpose and intended nature of the business relationship and, in higher risk situations, obtaining further information. In addition, banks should take measures to comply with national and international sanctions legislation by screening the customer's and beneficial owner's names against the UN and other relevant sanctions lists. The amount and type of information obtained, and the extent to which this information is verified, must be increased where the risk associated with the business relationship is higher. It may also be simplified where the risk associated with the business relationship is lower. (Financial Crimes Enforcement Network, 2016)

Enhanced Due Diligence (EDD) entails, first, obtaining additional identifying information from a wider variety or more robust sources and using the information to inform the individual customer risk assessment. Second, it involves carrying out additional searches (e.g., verifiable adverse media searches) to inform the individual customer risk assessment. Third, commissioning an intelligence report on the customer or beneficial owner to understand better the risk that the customer or beneficial owner may be involved in criminal activity. Fourth, verifying the source of funds or wealth involved in the business relationship to be satisfied that they do not constitute the proceeds from crime. And, finally, seeking additional information from the customer about the purpose and intended nature of the business relationship. (Federal Financial Institutions Examination Council BSA/AML InfoBase, 2017) All this of course burdens financial institutions with significant customer surveillance and financial costs, in addition to fueling the claim that financial institutions are being conscripted into "agents of the surveillance state."

The AML authorities, of course, would answer that where appropriate, banks could apply Simplified Due Diligence (SDD), which entails obtaining less information (e.g., not requiring information on the address or the occupation of the potential client), and/or seeking less robust verification, of the customer's identity and the purpose and intended nature of the business relationship; and, postponing the verification of the customer's identity, as needed. However, after conducting a holistic assessment of ML/TF risk, and where banks cannot apply the appropriate level of CDD, banks should not enter the business relationship or terminate the business relationship. In other words, the burden of proof would lie with the banks, which further adds to the level of pressure financial institutions feel under the present AML/CFT rules and regulations. (Financial Action Task Force, 2017)

16. Ongoing Consumer Due Diligence (CDD) Monitoring

Of course, CDD does not end here with banks simply knowing who their customers are. Ongoing CDD monitoring is expected by banks. Ongoing monitoring means the scrutiny of

transactions to determine whether those transactions are consistent with the bank's knowledge of the customer and the nature and purpose of the banking product and the business relationship. Monitoring also involves identifying changes to the customer profile (for example, their behavior, use of products and the amount of money involved), and keeping it up to date, which may require the application of new, or additional, CDD measures.

In fact, monitoring transactions is an essential component in identifying transactions that are potentially suspicious. Monitoring should be carried out on a continuous basis or triggered by specific transactions. It could also be used to compare a customer's activity with that of a peer group. It need not require electronic systems, although for some types of banking activity, where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions. Banks should adjust the extent and depth of monitoring in line with their institutional risk assessment and individual customer risk profiles. It is expected that enhanced monitoring would be required for higher risk situations, while banks may decide to reduce the frequency and intensity of monitoring where the risks are lower.

To be on the safe side, banks should document and state clearly the criteria and parameters used for customer segmentation and for the allocation of a risk level for each of the clusters of customers. Criteria applied to decide the frequency and intensity of the monitoring of different customer segments should also be transparent. To this end, banks should properly document, retain and communicate to the relevant personnel the results of their monitoring as well as any queries raised and resolved. If a bank suspects, or has reasonable grounds to suspect, that funds are the proceeds of crime or are related to terrorist financing, it shall report its suspicions promptly to the relevant Financial Intelligence Unit (FIU). Banks should flag unusual movement of funds or transactions for further analysis. Banks should have appropriate case management systems so that such funds or transactions are scrutinized in a timely manner and a determination made was to whether the funds or transaction are suspicious. Funds or transactions that are suspicious should be reported promptly to the FIU and in the manner specified by the competent authorities. The processes banks put in place to escalate suspicions and, ultimately, report to the FIU, should reflect this. While the policies and processes leading banks to form a suspicion can be applied on a risk-sensitive basis, a bank should report once ML/TF suspicion has formed. Naturally, adequate bank internal controls are a prerequisite for the effective implementation of policies and processes to mitigate ML/TF risk. (Australian Transaction Reports and Analysis Centre, 2017)

17. Bank Governance

Bank internal controls include: appropriate governance arrangements where responsibility for AML/CFT is clearly allocated; controls to monitor the integrity of staff compliance (in accordance with the applicable local legislation, especially in cross-border situations and the national risk assessment); and, controls to test the overall effectiveness of the bank's policies and process to identify, assess and monitor risk. In that regard, senior management should: promote compliance as a core value of the bank by sending a clear message that the bank will

not enter into, or maintain, business relationships that are associated with excessive ML/TF risks which cannot be mitigated effectively; implement adequate mechanisms of internal communication related to the actual or potential ML/TF risks faced by the bank; decide on the measures needed to mitigate the ML/TF risks identified and on the extent of residual risk the bank is prepared to accept; and lastly, senior management should adequately resource the bank's AML/CFT unit.

To mitigate ML/TF risk, senior management should: receive sufficient, regular and objective information to get an accurate picture of the ML/TF risk to which the bank is exposed through its activities and individual business relationships; receive sufficient and objective information to understand whether the bank's ML/CFT controls are effective (for example information from the Chief Compliance Officer on the effectiveness of control, or audit reports); and lastly, should ensure that processes are in place to escalate important decisions that directly impact the ability of the bank to address and control risks.

It is also important that responsibility for the consistency and effectiveness of AML/CFT controls be clearly allocated to an individual of sufficient seniority within the bank to signal the importance of ML/TF risk management and compliance, and that ML/TF issues are brought to senior management's attention. This includes, but is not restricted to, the appointment of a skilled compliance officer at management level. A bank's internal control environment should be conducive to assuring the integrity, competence and compliance of staff with relevant policies and procedures. (Federal Financial Institutions Examination Council BSA/AML InfoBase, 2017)

18. Vetting, Recruitment, Remuneration, Training and Awareness

Of course, internal controls extend well beyond governance. Banks should check that staff they employ have integrity and are adequately skilled and possess the knowledge and expertise necessary to carry out their function, where staff are responsible for implementing AML/CFT controls. The level of vetting procedures of staff should reflect the ML/TF risks to which individual staff are exposed and not focus merely on senior management roles. Steps should be taken to manage potential conflicts of interest for staff with AML/CFT responsibilities.

Bank staff training and awareness should be of high quality, and relevant to the bank's ML/TF risks, business activities and up to date with the latest legal and regulatory obligations, and internal controls. This training should be obligatory for all relevant staff, and tailored to lines of business within the bank, equipping staff with a sound understanding of specialized ML/TF risks they are likely to face and their obligations in relation to those risks. Training should have the desired effect, and this can be checked for example by requiring staff to pass tests or by monitoring levels of compliance with the bank's AML/CFT controls and applying appropriate measures where staff are unable to demonstrate the level of knowledge expected. In addition, AML/CFT training should be regular, relevant and not be a one-off exercise when staff are hired, and complemented by AML/CFT information and updates that are disseminated to relevant staff as appropriate. (Jersey Financial Services Commission, 2017)

19. Assessment of Controls

Banks should also take steps to be satisfied that their AML/CFT policies and controls are adhered to and effective. To this end, their controls should be monitored on an ongoing basis by the bank's compliance officer. In addition, the adequacy of and compliance with banks' AML/CFT controls should be reviewed by an audit function. Of course, it should be noted that banks are required to appoint a compliance officer at management level. In addition to advising relevant staff how to meet their obligations, their role should be to monitor and assess ML/TF risks across the bank as well as the adequacy and effectiveness of the measures the bank has put in place to mitigate the risks. The compliance officer should therefore have the necessary independence, authority, seniority, resources and expertise to carry out these functions effectively, including the ability to access all relevant internal information (including across lines of business, and foreign branches and subsidiaries).

Banks are required to have an independent audit function to test the bank's AML/CFT program with a view to establishing the effectiveness of the bank's overall AML/CFT policies and processes and the quality of its risk management across its operations, departments, branches and subsidiaries, both domestically and, where relevant, abroad. The findings should inform senior management's view of the design and implementation of the bank's AML/CFT framework. (Reserve Bank of New Zealand, 2017)

20. Financial Inclusion (FI)

Despite the effort to mitigate the cost to financial institutions for their participation in AML/CFT efforts through this Risk Based Approach (RBA), financial institutions and banks have complained stridently about the additional financial and administrative burden placed upon them by the existing AML/CFT regime. At the same time case after case of money laundering was brought against major financial institutions including: BNP Paribas (2014), HSBC Holdings (2012), BCCI (1991), Standard Charter (2012), Wachovia (now part of Wells Fargo) 2010, just to name a few. Given the Herculean task of monitoring billions of financial transactions daily and to encourage the financial sector to cooperate with state authorities in their AML/CFT efforts, for without the cooperation of the financial intermediaries any AML/CFT effort is bound to fail, state authorities endorsed the Global Partnership for Financial Inclusions (GPFI) at the G-20 summit in South Korea in 2010.

Financial Inclusion (FI) focuses on facilitating access to formal services for financially excluded and underserved groups, including low income, rural sectors, and undocumented groups. FI focuses on developing countries where the challenge is the greatest. The idea here was to entice the financial institutions to participate more willingly in AML/CFT efforts with the possibility of expanding their markets by "banking the un-banked" which constitutes approximately 50% of the world's adult population. The underlying premise of this initiative is that financially excluded and underserved groups, including low income, rural sector and undocumented groups, in both developing and developed countries should not be automatically classified as presenting lower risk for ML/TF. Consequently, the RBA which is now a central element of AML/CFT must now take into consideration the risks of financial exclusion and the benefits of bringing people into the formal financial system.

The general principle of RBA is that where there are higher risks, countries must require financial institutions to take enhanced measures to manage and mitigate those risks, and that correspondingly where the risks are lower (and there is no suspicion of money laundering or terrorist financing) simplified measures may be permitted. Financial Inclusion (FI) would then take the different steps of the AML/CFT process: Customer Due Diligence (CDD), record-keeping requirements, report of suspicious transactions, use of agents, and internal controls, and for each of them presents how the Standards can be read and interpreted to support FI. (Financial Action Task Force, 2017)

21. Risk Based Approach (RBA), Customer Due Diligence (CDD), and Financial Inclusion (FI)

For AML/CFT purposes, it is essential that financial products and services are provided through financial institutions subject to adequate regulation in line with the FATF Recommendations. Approximately 2.5 billion adults worldwide lack access to a formal bank account, which amount to 50% of the world's adult population. Combining RBA, CDD, and FI is no easy matter. Countries usually define the "reliable, independent source documents" which can be used to verify customers' identity; and financial institutions can also define a risk based approach with verification processes proportionate to ML/TF risk.

FATF allows for Simplified (though neither an absence nor an exemption from) CDD measures where there is a lower risk of ML/TF. Simplified DCC standards can be decided at country level, based on risk or at financial institution level; the principle remaining that each financial initiation must know: who their customers are, what they do, and whether they are likely to be engaged in criminal activity or be conduits for proceeds of crime. In a RBA, it would be acceptable for a financial institution to infer the purpose and intended nature of the business relationship from the type of transaction or business relationship established.

Ongoing CDD and business relationship monitoring must be performed through manual or electronic scanning. Technology has also paved the way for anti-money laundering software, that detects large increases in account balances or large withdrawals, and which filters data and classifies it per levels of suspicion. Software is also used to detect transactions with banking institutions in blacklisted or hostile countries. When such transactions are identified, the program alerts bank managers who then study the information and decide whether it should be reported to the government. FI would thus not reduce CDD, since RBA is allowed, with the degree of monitoring based on the risks associated with a customer, an account, and products or services used. Regulatory authorities are to be mindful and give due weight to determinations (monetary or other thresholds, to be reviewed regularly) made by financial institutions. Monitoring to detect unusual, potential suspicious transactions is required, with any actual suspicion leading to the removal of any threshold or exception. Simplified CDD could be mitigated by closer transaction monitoring, acknowledging however that an absence of sufficient information due to too little CDD could limit the utility of monitoring.

It is required that financial institutions keep at least the information on identification documents for a minimum of five years. Options available are scanning of documents, or keeping electronic copies, or merely recording reference details. Of course, an RBA is usually

not applicable to suspicious activity reporting. But an RBA could be appropriate for identifying suspicious activities. Transactions with vulnerable groups are usually not subject to separate or specific monitoring, but some financial institutions have developed specific indicators to identify suspicious activities. Agents may be permitted, in effect or practice, to perform identification and verification obligations, the prevalent rule being that financial institutions hold the business relationship and are accountable for it, and ultimately liable with respect to agents' compliance with AML/CFT requirements. It is recommended to balance regulatory concerns about agents with the financial inclusion objective. Finally, transaction monitoring systems must cover what is performed by agents. The overall goal being to ensure that financial inclusions (FI) and AML/CFT objectives mutually reinforce each other. (Financial Action Task Force, 2017)

22. Unintended Consequences of AML/CFT Risk-Based Approach (RBA) and Financial Inclusion (FI)

Unfortunately, in the real world very little goes as planned. Per the International Monetary Fund (IMF), global money laundering transactions are estimated at 2-5% of global GDP, or roughly $1-2 trillion U.S. Dollars. Yet, per the United Nations Office on Drugs and Crime (UNODC), less than 1% of global illicit financial flows are currently seized by authorities. Every year money laundering channels around $2 trillion worth of proceeds from various illicit activities. (PWC Global, 2017) This clearly is a case of market failure and represents an economic inefficiency which can only be addressed by state authorities with the cooperation of the private sector, i.e., financial institutions, and society at large.

Unfortunately, the present AML/CFT approach has been of very limited success despite successive detailed and legalistic enforcement and assessment guidance mandated by FATF over the years. As stated earlier, and from a historical perspective, society has been more tolerant of money laundering given the perception of it being a "white collar" or "victimless" crime resulting primarily from fraud. This began to change with the widespread use of illicit drugs and the ensuing "war on drugs" which greatly increased global money laundering although fraud still remains the main source of illicit funds transactions to the present day. As nations, primarily in North America and Europe, confronted this growing global phenomenon, a more multilateral approach was called for with various United Nations Conventions against corruption and Illicit Drug Trafficking. This multilateral approach was reaffirmed with the end of the Cold War and with terrorism emerging as the number one threat to the global order as states led by the USA, under the auspices of the OECD and other international agencies such as the UN, turned their attention to this growing threat. The main spearhead of this effort was the Financial Action Task Force (FATF) which originally was geared towards anti-money laundering (AML) but then turned its attention quickly to combating the financing of terrorism (CFT) following the September 11, 2001, terrorist attacks on New York and Washington, DC. One could argue that it was a mistake to co-mingle separate objectives with one policy tool but that is an issue that is beyond the scope of this paper. The problem was further accentuated when "sanctions violations" were also added to the list of objectives to hinder nuclear proliferation. What is clear is that the present AML/CFT approach has had miniscule impact on illicit financial flows given the enormous resources expended and

furthermore has had unintended consequences that further weakens its effectiveness.

It soon became clear that the original FATF Recommendations for AML/CFT were too onerous and all-encompassing with most of the financial burden placed on financial institutions. The costs of compliance were enormous in comparison to the benefit even with the "war on terrorism" superseding the more relaxed "war on drugs", although the latter was onerous in comparison to the even more relaxed efforts against the more widespread "white-collar" crime of fraud. Given the push-back from both the financial industry as well as concerns raised among civil liberties groups and other critics surrounding the data privacy rights of citizens following the passage of The Patriot Act, the authorities moved to ease the burden of compliance with the FATF Recommendations by introducing the Risk-Based Approach (RBA) as detailed previously. This was presented as a more efficient and palatable, i.e., a less costly and less intrusive a process for financial institutions, although, ultimately financial institutions remained fully responsible for customer due diligence (CDD) compliance. This "offer" was then sweetened with the prospect of financial inclusion (FI). Namely, a concerted effort on the part of state authorities to bring into the formal financial markets the 50% or more of the world's "un-banked" population, thus expanding the pool of potential bank customers that were still without a bank account! It was understood that no matter how intense the oversight of the financial system, you are still missing the significant amount of financial flows that take place in the informal sector of the economy, especially the underground economy. You cannot monitor what is not recorded or what is not observable! This was then presented as a "win-win" solution with the banks being able to meet their responsibilities as far as compliance with the AML/CFT regulations as well as being more than compensated with "financial inclusion (FI)", i.e., a significant expansion of the banking market. In fact, this was an illusion as financial institutions remained fully responsible for all their customers' financial activities under the now combined RBA/FI approach.

23. AML/CFT Risk-Based Approach (RBA) and Financial Exclusion (FE)/ "De-Risking"

No doubt Adam Smith would wonder at this point in our time line if the actors involved in this play had read his accounts of the "invisible hand" and the "rationing function of markets". This is by no means an effort to make light of the seriousness of money laundering, terrorism financing, and sanctions violations by individuals, banks, and other financial entities. These are serious offenses with significant negative consequences for all nations, rich and poor. In fact, the FATF inspired international efforts to combat money laundering and combat the financing of terrorism are a necessary step towards increasing the safety of the financial system and enhancing security.

Country compliance with the AML/CFT international standard plays an important role in enhancing the world's financial system integrity. Yet, the IMF argues that the compliance with the AML/CFT standard is low. At least one IMF report finds that only a few countries (primarily high income countries) comply to a larger degree with the AML/CFT standard. More generally, the report reveals widespread weak compliance by financial institutions and the adverse impact on financial transparency created by the cumulative effects of poor

implementation of standards on customer identification in the financial sector (banks) and non-financial businesses and professions (non-banks), as well as standards on entity transparency (ownership and control of firms and trusts). (Yepes, 2011)

In fact, the most recent FATF (2016) report gave the U.S., that views itself as a standard setter among nations, failing scores for its efforts to prevent the laundering of criminal proceeds by shell companies, accountants and real estate agents. Overall, the U.S. is more effective in countering terrorism financing, but does not do enough to rein in corporate secrecy, presenting serious gaps in law enforcement efforts that leave the financial system vulnerable to dirty money. The report scored the U.S., "non-compliant" (the lowest possible score) on its ability to determine the true owners of shell companies. It also gave the U.S. a failing score for its minimal monitoring of non-financial industries, such as law firms and realtors. These are the same shortcomings raised in FATF's last evaluation of the U.S. in 2006. (Wolf, 2016)

Banks have from the start complained about the rising costs of compliance with AML/CFT standards. On the one hand, there are regulators that have raised the bar and their expectations when it comes to the measures used by financial institutions to prevent and detect suspicious transactions, and on the other hand, there are laws and regulations. Without a doubt, the cost of compliance is growing around the world and this higher compliance spending has affected bank profits negatively. With global banks being hit with multi-billion dollar fines in recent years, there has been a lot of pressure from regulators for greater spending on compliance. (Trulioo, 2016) Ongoing requirements in transactions monitoring, Know Your Customer (KYC), and talent management are raising compliance costs and keeping them high. This has resulted in a surge in demand for bank compliance officers, as financial institutions scramble to quickly fill a huge gap in knowledge, expertise, and manpower. Notwithstanding the reluctance of career bankers to undertake these positions that leave them vulnerable to being set-up as the "fall guy", financial institutions are also scrambling to adopt automated processes using sophisticated software to handle the know your customer (KYC) function. (Accenture Consulting, 2015)

Under the present approach to AML/CFT, banks are required to prevent sanctions violations and assess and mitigate money laundering and terrorist financing risks, or face severe penalties. This has led banks to adopt a conservative position with respect to their customers. This includes no longer providing services to firms, market segments, and countries seen as being a higher risk and that could be cause of costly future fines, monitoring, or even prosecutions. Rather than adopting the Risk-Based Approach (RBA) to AML/CFT with the prospect of being rewarded with an expanded customer base resulting from Financial Inclusion (FI), banks are choosing to cease to engage in certain activities completely, rather than judging the risks of clients on a case-by-case basis, i.e., banks are engaging in "de-risking". (Ramachandran, 2015)

The fact that de-risking has and does happen was reaffirmed by a report published by the Financial Conduct Authority (FCA), namely that banks have been and continue to engage in de-risking by refusing to open new or closing existing customer accounts. It appears that from a cost and risk-based approach the most efficient option to mitigate anti-financial crime

(AFC) risks would be to avoid them altogether or end those relationships where the cost of applying controls outweighs the financial benefit gained over the long-term business relationship. The report identifies the main explanatory variables behind de-risking as the higher costs of compliance, stricter regulatory requirements and the deterrent effect created because of criminal, civil and regulatory prosecutions and penalties. The sectors most adversely affected by de-risking are: money service businesses (MSBs), pawnbrokers, charities, foreign embassies, nonprofit organizations (NPOs), and financial technology companies. (Sheen, 2017)

A further consequence of de-risking has been a contraction of correspondent banking and other interbank relationships. Reports by both the Bank for International Settlements (BIS) and the International Monetary Fund (IMF) emphasis the effect of de-risking on the correspondent banking system. Through correspondent banking relationships, banks can access financial services in different jurisdictions and provide cross-border payment services to their customers, supporting international trade and financial inclusion. Growing evidence indicates that some banks providing these services are reducing the number of relationships they maintain and are establishing few new ones. This implies a threat that cross-border payment networks might fragment and that the range of available options for these transactions could narrow. To avoid penalties and the related reputational damage correspondent banks have cut back services for respondent banks that, first, do not generate sufficient volumes to overcome compliance costs; second, are in jurisdictions perceived as very risky; or lastly, choose to provide payment services to customers about which the necessary information for an adequate risk assessment is not available. (Committee on Payments and Market Infrastructures, 2015)

Another IMF report has concluded that correspondent banking relationships (CBRs), have been terminated outright in some jurisdictions following the recent global financial crisis. Surveys and other available evidence indicates that smaller emerging markets and developing economies in Africa, the Caribbean, Central Asia, Europe and the Pacific as well as countries under sanctions may be the most affected. AML/CFT efforts are of course not the only considerations for individual banks in deciding to withdraw CBRs. Other considerations include the new macroeconomic environment, changes in the regulatory and enforcement landscape, economic and trade sanctions, and tax transparency. Further pressure to withdraw CBRs could disrupt financial services and cross-border flows, including trade finance and remittances, potentially undermining financial stability, inclusion, growth, and development goals. (International Monetary Fund, 2016)

Low profit, reputational concerns, and rising AML/CFT scrutiny contribute to de-risking, which can further isolate communities from the global financial system and undermine AML/CFT objectives. These closures have had a multiplier effect on financial access for the individuals and groups served by those businesses, including significant humanitarian, economic, political, and security implications. This financial exclusion has resulted in effectively cutting access to finances, further isolating communities from the global financial system, exacerbating political tensions, and potentially facilitating the development of parallel underground “shadow markets”, thus further undermining the AML/CFT objectives.

(Shetret, 2015) According to a World Bank report, the introduction of AML/CFT regulations may have had the unintended and undesirable consequence of reducing the access of low income people to formal financial services. (Egwuagu, 2005) This consequently has had a disproportional effect on developing economies and in particular the "poorest" economies of the world that are the least connected to the global financial structure.

Multinational organizations such as the IMF and the World Bank together with numerous NGOs have suggested that improvements to the present AML/CFT system are warranted. This would include a more rigorous assessment of the unintended consequences of the AML/CFT system and sanctions enforcement at both the global and national levels with attention on the impact on low-income groups and countries. More and better data should be generated and shared to assess the unintended consequences of AML/CFT. Although, the risk-based approach should be applauded, it needs to be applied more extensively and more consistently. Simplified due diligence should be further encouraged where it is in the best interests of transparency. Not all financial transactions and not all bank customers represent equal risk and it would be inefficient to treat them that way. Yet while the level of uncertainty faced by banks is at an all-time high, there is a need to strengthen and align the regulatory and supervisory frameworks which can only be achieved if there is a political buy-in by national governments to adopt necessary reforms. This is no easy task as it also requires the buy-in by both bank and nonbank financial institutions. To that end national governments need to invest in supervisory capacity to ensure compliance with the Basel Core Principles for Effective Banking Supervision and the FATF Recommendations, and to increase the exchange of beneficial ownership information. To mitigate the cost of compliance, national governments and financial institutions should accelerate the adoption of new technology that would reduce the cost of customer identification, know your customer (KYC) compliance, and customer due diligence (CDD).

References

About Business Crime Solutions Inc. (2017). *About Business Crime Solutions Inc.* Retrieved from https://www.moneylaundering.ca

Accenture Consulting. (2015). *Reducing the cost of anti-money laundering compliance.* Retrieved from https://www.accenture.com

Alliance, D. P. (2016). *Drug War Statistics*. Retrieved from http://www.drugpolicy.org/drug-war-statistics

Australian Transaction Reports and Analysis Centre. (2017). *Ongoing Customer Due Diligence (OCDD).* Retrieved from www.austrac.gov.au

Basel Committee on Banking Supervision. (2014). *Sound Management of Risks Related to money Laundering and Financing of Terrorism.* Retrieved from www.bis.org

Borrero, A. M., & Errico, L. (2017). *Offshore Banking: An Analysis of Micro- and Macro-Prudential Issues.* Retrieved from https://www.imf.org

Campbell, R., & McConnell, S. L. (2015). *Macroconomics: Principles, Ploblems, and Policies.* New York: McGraw-Hill Education.

Committee on Payments and Market Infrastructures. (2015). *Correspondent Banking.* Basel: Bank for International Settlements.

Crime, U. N. (2011). *Estimating Illicit Financial Flows Resulting From Drug Trafficking and Other Transnational Organized Crimes*. Retrieved from http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf

Currency, O. O. (2016). *Bank Secrecy Act*. Retrieved from https://www.occ.gov/topics/compliance-bsa/bsa/index-bsa.html

Egwuagu, R. H. C. (2005). *AML/CFT Regulation: Implications for Financial Service Providers that Serve Low-income People*. Washington DC: World Bank.

El-Qorchi, M. (2002). The Hawala System. *Finance and Development, 39*(4). Retrieved from https://www.gdrc.org

FATF(12). (Updated 2016). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.* Retrieved from www.fatf-gafi.org/recommendations.html

FATF. (2017). *FATF Members and Observers*. Retrieved from www.faft-gafi.org

FATF. (2017). *Financial Action Task Force*. Retrieved from www.fatf-gafi.org

FATF. (2017). *High-Risk and Non-Coopertive Jurisdictions*. Retrieved from www.faft-gafi.org

Federal Financial Institutions Examination Council BSA/AML InfoBase. (2017). *BSA/AML Risk Assessment*. Retrieved from https://www.ffiec.gov

Financial Action Task Force. (2005). *Money Laundering & Terrorist Financing Typologies 2004-2005*. Paris: FATF Secretariat, OECD.

Financial Action Task Force. (2017). *FATF Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion.* Retrieved from www.fatf-gafi.org

Financial Action Task Force. (2017). *FATF Recommendation 5: Customer due diligence and record-keeping.* Retrieved from https://www.un.org

Financial Crimes Enforcement Network. (2016). *Customer Due Diligence Requirements for Financial Institutions.* Retrieved from https://www.federalregister.gov

Financial Crimes Enforcement Network. (2017). *History of Anti-Money Laundering Laws*. Retrieved from https://www.fincen.gov

Financil Action Task Force. (2014). *Guidance for a Risk-Based Approach: The Banking Sector*. Paris: FATAF Secretariat.

FindLaw. (2016). *White Collar Crime*. Retrieved from FindLaw.

Global Financial Integrity. (2017). *Tax Havens/Bank Secrecy.* Retrieved from http://www.gfintegrity.org

Greco, J. F. (2017). *Multinational Finnacial Management, Alan Shapiro* (7th ed.). Retrieved from www.siue.edu

IMF. (2017). *Offshore FinancialCenters.* Retrieved from https://imf.org

International Monetary Fund. (2016). *The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action.* Washington DC: International Monetary Fund.

Investigation, F. B. (2016). *White-Collar Crime*. Retrieved from https://www.fbi.gov/investigate/white-collar-crime

IRS. (2016). *Bank Secrecy Act.* Retrieved from https://www.irs.gov/businesses/small-businesses-self-employed/bank-secrecy-act

Jersey Financial Services Commission. (2017). *Vetting Awarenesss and Training of Employees.* Retrieved from https://www.jerseyfsc.org

Kodres, L. E. (2017). *What is Shadow Banking?* Retrieved from www.imf.org

Legal Dictionary. (2017). *Money-Laundering*. Retrieved from https://legaldictionary.net/money-laundering/

Management, S. D. (2016). *USA Patriot Act.* Retrieved from http://searchdatamanagement.techtarget.com/definition/Patriot-Act

Payan, T. (2013). *A War That Can't be Won.* Tucson: The University of Arizona Press.

PWC Global. (2017). *Anti-Money Laundering: Global Economic Crime Survey 2016*. Retrieved from http://www.pwc.com

Ramachandran, C. L. (2015). *Unitended Consequences of Anti-Money Laundering Policies for Poor Countries.* Retrieved from https://www.cgdev.org

Reserve Bank of New Zealand. (2017). *Countries Assessment Guideline*. Retrieved from www.rbnz.govt.nz

Sheen, S. (2017). *Review of the Derisking Report Prepared for the Financial Conduct Authority ("FCA").* Retrieved from http://www.acams.org

Shetret, T. D. (2015). *Undertstanding Bank De-Risking and its Effects on Financial Inclusion.* London: Global Center on Cooperative Security.

Sullivan & Cromwell LLP. (2016). *2015 Year-End Review of BSA/AML and Sanctions Developments and Their Importance to Financial Institutions.* New York: Sullivan & Cromwell LLP.

The Economist. (2017). *How Does Bitcoin Work?* Retrieved from http://www.economist.com

The World Bank. (2017). *Nonbanking Financial Institution*. Retrieved from http://www.worldbank.org

Treasury, U. S. (2015). *National Money Laundering Risk Assessment 2015.* Washington DC: US Government.

Trulioo. (2016). *Are Compliance Costs Breaking Banks?* Retrieved from https://www.trulioo.com

U.S. Department of the Treasury. (2015). *National Money Laundering Risk Assessment 2015.* Washington, DC: www.treasury.gov.

U.S. Department of the Treasury. (2017). *Hawala and Alternative Remittance Systems*. Retrieved from https://www.treasury.gov

Whitehead, H. (2017). *Top 5 Money laundering Cases of the Last 30 Years*. Retrieved from http://www.int-comp.com

Wolf, J. S. (2016). *Business News*. Retrieved from http://www.reuters.com

Yepes, C. V. (2011). *IMF Working Paper*. Retrieved from www.imf.org

Copyrights