

Working Paper

Anti-Money Laundering

From Prevention To Prosecution

By

Jeff Rooney

Risk Management and Compliance

JSD (candidate), Doctorate of Juridical Sciences of Law and

JSM, Master of Juridical Sciences of Law

August 14, 2011

Published by:

JD Supra, LLC | 501 Bridgeway Sausalito, CA 94965

Table of Contents

1. AML – Introduction	3
2. AML – Take Away Thy Privacy	4
3. AML – Tough Offshore Legislation	5
4. AML – A United States Project	6
5. AML – An International Project	7
6. AML – Success or Mess	8
7. AML – FinCEN Investigation	9
8. AML – Prosecution	12
9. AML – Conclusion	13

1. AML – Introduction

Since the terrorist attacks on the World Trade Center on September 11, 2001 (“9/11”), worldwide legislation for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) has taken on heightened levels of security.

Six weeks after the 9/11 attacks, on October 24, 2001, the U.S. bureaucrats agreed to enact the U.S. Patriot Act to combat all acts of money laundering and terrorist financing¹ as well as enacting strict code of standards for International Trade and Business with the United States. This codification entailed the sanctioning of any country from doing business with the U.S. if they did not have acceptable legislation that cooperatively pursued and supported the same AML/CFT objectives. Countries such as North Korea, Cuba, Iran, Burma, Sudan, Syria, Zimbabwe, Congo, Belarus, Lebanon, and Somalia have been sanctioned from the U.S. and regulations are enforced not allowing any kind of business with these high-risk countries.²

The U.S. Patriot Act has approximately 300 pages of legislation that has positively influenced the international communities to adopt AML/CFT standards requiring financial institutions to implement AML/CFT programs used to identify, detect, and prevent money laundering or any other unlawful activities that would threaten global economic and financial systems.

There are many but similar definitions for money laundering, but the most comprehensive is defined in Article 1 of the European Communities Directive of 1990. Money laundering is:

“the conversion or transfer of property, knowing that such property is derived from serious crime, for the purpose of concealing or disguising the illicit origins of the property or of assisting any person who is involved in committing such as offense or offenses to evade the legal consequences of his action, and the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from serious crime.”³

The European Communities Directive asserts a powerful definition for money laundering by using “serious crime” as a legal acquiescence or a protective shield that is impossible to penetrate. Other words, the criminal activity of money laundering cannot be interpreted or even argued to be either a minor or moderate offense. Under Article 1, the definition of money laundering provides an overall interpretation and consequence that is always the same – that is, money laundering is a serious crime. For example, “when credit and financial institutions are used to launder proceeds from criminal

¹ “Amlid Database - USA Patriot Act 2001,” *H.R. 3162*, November 2010, https://www.imolin.org/doc/amlid/USA_Patriot_Act.pdf.

² “31 CFR - Money and Finance,” *Chapter V -- Office of Foreign Assets Control*, November 2010, http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?sid=39557f936e511fe5484b63a5e869412f&c=ecfr&tpl=/ecfrbrowse/Title31/31cfrv3_02.tpl#1000.

³ “Financial Money Laundering | Money Laundering Law Essay | Law Teacher,” November 2010, <http://www.lawteacher.net/money-laundering/essays/financial-money-laundering.php>.

activities whether perceived as minor, moderate or serious will always have a negative influence on the soundness and stability of the institution”⁴ -- that is, it increases the negative concern and confidence in the financial system, and as a whole, will lose the trust of the public. Although the AML/CFT provisions and programs have made great achievements in the monitoring and controlling of money laundering and terrorist financing, but it has come down to the loss of financial privacy.

2. AML – Take Away Thy Privacy

Privacy for criminals is a vital requirement that needs to be maintained in order for their criminal activities not to be identified by law enforcement authorities. For a criminal, privacy is the means of creating sophisticated schemes for “covering-up” their illegitimate business activities and personal identities. It is in their best interest to conduct their illicit activities with the highest level of privacy, caution, and discretion so that nothing is tracked or audited backed to them. To mitigate and protect their privacy and illegal wealth, criminals may consider and implement some of the following schemes:

1. Criminals will investigate and visit banks in jurisdictions that don’t comply with AML/CTF regulations, customer due diligence requirements or the provisions set by their nation and the Financial Actions Task Force (FATF). For example, the countries of **Argentina, Bangladesh, Cameroon, and Iran**⁵ are nations that have either “no” or “partial” compliance with the FATF and AML/CFT regulations.
2. Criminals will try to establish one or more offshore banks accounts that have privacy laws. When this is done correctly, the laundered money and investments that appears to be legitimate will be much more secure from almost all legal claims and investigations based in the U.S. and other countries if there is no evidentiary fact that demonstrates it to be suspect or illegal.
3. Criminals will never sign a suggested waiver of privacy rights. If a financial institution (e.g., a casino) asks for such a waiver, money launderer’s will leave immediately and look for another bank.⁶
4. Criminals will not open an account at a foreign branch of a U.S. bank, or at a foreign bank that has U.S. branches. Under the Bank Secrecy Waiver, offshore banks are immediately under the jurisdictions of the U.S. courts that open-up the opportunities for U.S. law enforcements to penetrate offshore bank secrecy and privacy laws to gather evidence that can be used to prosecute and convict criminal suspects.⁷

⁴ “European Communities Directive of 1990,” *Prevention of Financial Systems used for Money Laundering*, November 2010, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0308:EN:HTML>.

⁵ “Country Profiles - Anti-Money Laundering,” *Lack of Transparency*, November 2010, http://www.estandardsforum.org/browse/standard?standard_id=13.

⁶ “TN.gov,” *Waiver of Privacy Rights*, November 2010, <http://www.tennessee.gov/sos/charity/gaming/ss-6063.pdf>.

⁷ “Bank Secrecy Waiver Agreements: The Confidentiality Exception,” *New money laundering legislation and strategies*, November 2010, http://www.escapeartist.com/Offshore/Articles/Bank_Secrecy_Waiver/.

5. Criminals will try to use attorney-client privilege in the attempt to protect the privacy of consultations with or under the direction of an attorney. Substantial privacy can be obtained when criminals conduct business and financial transactions through an attorney. If the consulting attorney has not been criminally influenced, “attorneys are prohibited from offering advice that would result in or encourage the administration of a crime” and to enforce this oath there are some jurisdictions, not including the U.S., that require attorneys to report their clients to local law enforcement authorities (e.g., BVI and the Cayman Island) of “suspicious transactions” that are alleged to be illegal. Caribbean jurisdictions require attorney’s to comply with AML legislation and reporting suspicious transactions.⁸

6. There are smart criminals that will not use offshore accounts to hold U.S. securities. If they did, that would open-up a major hole in their protection for privacy because the U.S. Patriot Act gives its law enforcement authorities the right to demand the identity of individuals with a “correspondent account” and who have customers with an offshore bank account holding an invested interest in U.S. securities purchased with U.S. dollar denominations.

There are some cases where the U.S. government has confiscating correspondent accounts under the notorious “civil forfeiture” statutes. Also, there is the Internal Revenue Service (IRS) qualified intermediary (QI) regulations⁹ that involve correspondent accounts and U.S. depositories in foreign banks who purchase U.S. securities and then refuse to identify themselves to the IRS under the QI regulations. Under QI regulations, these correspondent accounts are subject to a 30 percent withholding tax not just on income from the account, but also on all “broker proceeds” when they sell.

3. AML – Tough Offshore Legislation

Ever since 9/11 and the rise of international AML/CFT programs, privacy is no longer a mandatory right. Under the watchful eye of the U.S. and other allied nations, government and law enforcement agencies have the authority to tap phone lines or emails, put key loggers on computers, and search offices, homes, and financial records of all kinds with ease if they have “reasonable doubt” of suspicious transactions that may be linked to money laundering or terrorism.

Recently, a key proposal for the amendment of the USA Patriot Act focuses on enhanced provisions that give U.S. intelligence agencies the full power to: 1) *conduct “roving” wiretaps without specifying a particular phone number or e-mail account;* 2) *force institutions to surrender credit, banking, medical, mental health and library records;* and 3) *spy on so-called lone-wolf foreign nationals, who have no affiliation to either terrorist organizations or foreign governments.*¹⁰

⁸ “IBA Anti-Moneylaundering Forum - Caribbean,” *Lawyers Guide to Legislation and Compliance*, November 2010, <http://www.anti-moneylaundering.org/Caribbean.aspx>.

⁹ “IRS - Qualified Intermediary,” n.d., <http://www.irs.gov/businesses/international/article/0,,id=102314,00.html>.

¹⁰ “Democrats vote to renew Patriot Act,” November 2010, <http://www.wsws.org/articles/2010/feb2010/patrf27.shtml>.

With the advances of AML/CFT technology such as, interconnected databases, e-commerce, and the International Money Laundering Information Network (IMoLIN), and Business Intelligence SAS systems the acts of money laundering within a financial institution has become very hard to accomplish.

Many offshore jurisdictions that were an attractive spot for money laundering has taken tough AML/CFT measures. Offshore jurisdictions once offered protection and preservation of financial privacy, but did so as a matter of law; anyone who violated that privacy could be punished with fines and jail terms. In many offshore jurisdictions such as, **Bermuda and the Cayman Islands** have demonstrated that only a court order can pry open the financial records of an individual or business, however, if they have “suspicious transactions” that may be related to criminal activities then under the Proceeds of Crime (AML/CFT) Regulations 2008¹¹ and Money Laundering Regulations 2009¹² that now take away those privacy rights once used by criminals.

Both Bermuda and the Cayman Islands have experienced recent changes to their laws where they now have more stringent AML/CFT measures. In comparison to the leaders of the U.S., the UK, and Australia in the fight against money laundering and the implementation of FATF 40 Recommendations, trust and financial services legislation, and KYC requirements now shows positive results where their AML/CFT programs “are not only keeping up with these leaders but in many cases are outdoing them.”^{13, 14}

4. AML – A United States Project

In the U.S., personal and commercial banking transactions were once considered to be of high integrity, unobtrusive, trustworthy, and morally conducted. Now banks and other financial institutions are now required to reveal anything and everything about a customer to the government if they detect any “suspicious activity” that reveals customer financial transactions to be related to unlawful activities. In the event an activity, a financial institution is required to report this information to the Financial Crimes Enforcement Network (FinCEN) and the names of any suspects that may be involved.

FinCEN then provides this data to more than 165 federal and local law enforcement agencies, from the FBI and the Secret Service down to the local sheriff and police departments. Even law enforcement agencies of foreign countries are allowed to have access to this proprietary information under certain conditions and international treaty laws.¹⁵

¹¹ “Bermuda - Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008,” November 2010, <https://www.imolin.org/amlid2/browse.jsp?country=BER>.

¹² “The Cayman Islands - Money Laundering Regulations 2009,” November 2010, <https://www.imolin.org/amlid2/browse.jsp?country=CAY>.

¹³ “IMF - Anti-Money Laundering/Combating the Financing of Terrorism,” *Detailed Assessment Reports by the IMF*, November 2010, <http://www.imf.org/external/np/leg/amlcft/eng/>.

¹⁴ “Caribbean Financial Action Task Force,” *Mutual Evaluation Reports - Bermuda and Cayman Islands*, November 2010, <http://www.cfatf-gafic.org/>.

¹⁵ “FinCEN What We Do,” *Who are FinCEN's Customers?*, November 2010, http://www.fincen.gov/about_fincen/wwd/faqs.html.

In a 2009 report, the Government Accountability Office (GAO) mentions that FinCEN makes protecting the privacy of SAR information received from financial institutions a top priority. FinCEN receives and shares millions of individual profiles and financial information with intelligence agencies that it's difficult to determine the extent that this proprietary information is shared, maintained, and internally controlled.¹⁶ Not knowing what the risks are of losing privacy is an important issue, and this is the absolute reason that explains why FinCEN has exempted itself from the Freedom of Information Act and the Privacy Act of 1974 that would otherwise permit disclosure of information to persons whose records are in its databases.¹⁷

5. AML – An International Project

With the high-level of financial security in all major nations makes it difficult for money launderer's and the financing of terrorism to be carried-out. In many cases, criminals will try to avoid this high-level of security by establishing criminal cells all over the world where they will wire-transfer illicit funds to multiple jurisdictions that have lenient AML/CFT legislation and controls.

Offshore jurisdictions that are vulnerable to money laundering, the financing of terrorism, and criminal organizations include **Angola, Antigua and Barbuda, Azerbaijan, Bolivia, Ecuador, Ethiopia, Greece, Indonesia, Kenya, Morocco, Myanmar, Nepal, Nigeria, Pakistan, Paraguay, Qatar, Sri Lanka, Sudan, Syria, Thailand, Trinidad and Tobago, Turkey, Turkmenistan, Ukraine and Yemen.**¹⁸

Organized crime, terrorism, and corruption are most often international and cross border in nature; combating these threats requires an international response. The Egmont Group has created an international alliance of 165 members that provides invaluable support to governments concerned with combating the threats posed by criminals, terrorists and corrupt officials – known as, Financial Intelligence Units (FIUs).

The Egmont Group defines their FIUs as a central, national agency responsible for receiving (as permitted per request) and disseminating analyzed financial data to competent authorities. The disclosures of typical information include:¹⁹

- Suspected proceeds of crime and potential financing of terrorism, or
- Information required by national legislation or regulation, in order to combat money laundering and terrorism financing.

¹⁶ "U.S. GAO - Bank Secrecy Act," *FinCEN Needs to Further Develop Its Form Revision Process for SARs*, November 2010, <http://www.gao.gov/new.items/d10609t.pdf>.

¹⁷ "USDOJ: Freedom of Information Act (FOIA)," November 2010, <http://www.justice.gov/oip/>.

¹⁸ "Proshare - UK Treasury alerts institutions on weak AML controls in Nigeria and other countries," November 2010, <http://www.proshareng.com/news/singleNews.php?id=11380>.

¹⁹ "Egmont Documents | The Egmont Group," *FIU Definition Interpretative Note*, November 2010, <http://www.egmontgroup.org/library/egmont-documents>.

FIUs at a minimum must be able to share information from financial disclosures and the results of their analysis regarding money laundering and related crimes, i.e., as determined by domestic AML/CTF legislation, competent authorities and, then with international FIUs. A critical element in assessing the dissemination and sharing of information involves determining the extent to which international laws permit the cooperation with other FIU members through the exchange of information.

6. AML – Success or Mess

As money laundering legislation and regulations has toughened across the globe, will it produce the results in money laundering prevention? Inevitably, money laundering is a huge problem and all financial markets, and their systems cannot produce effective outcome to identify and prevent it from occurring. The financial market is continuously evolving in the creation of financial products and strategies to make money as well as trying to bypass financial regulations.

When the financial industry creates new products and services, the legislation cannot keep pace and it allows for the creation of new unlawful opportunities. For many years, consumer protection and the lack of transparency has created opportunities for “Rogue Ponzi” and “Sub Prime Mortgage” schemes that helped to create today’s financial crisis. Thereafter, law enforcement and regulation finally catches up and enforces new legislation such as, the Dodd Frank Wall St. Reform and Consumer Protection Act in order to correct the mess that has been overlooked for the past 10-years.

While the characteristics of high risk-return investment opportunities that has driven the global markets are also the same characteristics that appeal to money launderer’s. On Wall Street, financial professionals are continuously mitigating and transferring risks in order to legitimately create opportunities that will yield positive returns and increase wealth; money launderer’s do the same thing but with illegitimate funds.

Although there are tremendous AML/CFT efforts taking place, such as regulatory compliance, Know Your Customer (KYC), and Suspicious Activity Reporting (SAR) it poses the question: Is AML/CFT regulations a success or a mess? Can AML/CFT regulations ensure that it will not damage the financial market it is supposedly there to protect?

The above questions are extremely difficult to answer, but I can argue that current AML/CFT regulations are inefficient, arbitrary, capricious, and unreasonable. Why? Because the regulations cannot control the freedom of the financial markets that allow money laundering to be successful, and the money launderer’s that get caught are those who are not financial professionals.

To overcome the problem of money laundering, the first step is to remove SARs that is “gagging” the financial system and replace it with a monetary tracking system. This system tracks the movement of cash denominations that are marked and digitally recorded. Illicit money that is not marked is flagged and confiscated. This efficient method changes the regulations for foreign currency exchange and

compliance regulations that require financial organizations to procure global transaction-monitoring solutions to aid the detection and prevention of money laundering, thereby helping to shift the onus away from law enforcement and onto financial organizations. Whereby, law enforcement does not get tied down by the examination and evaluation of global data sources and being restricted by the many international laws.

Since the Vienna Convention of December 19, 1988, AML regulations have gotten tougher, but on who? Is the AML global regime having an impact on the criminal activity of money laundering or is it merely getting tougher on those financial institutions required to comply with the multitude of regulations. An important point to remember is that the AML regulations were designed to deter, detect, and prosecute money launderer's, but will it ever achieve these asserted objectives? ²⁰

7. AML – FinCEN Investigation

FinCEN is an agency of the U.S. Department of Treasury that is responsible for setting policies to deter, detect money laundering activities. Under the Bank Secrecy Act (BSA) and the U.S. Patriot Act, it administers and improves on those statutes by acting as central location for collecting and interpreting the analysis of financial intelligence, and then sharing this intelligence with other law enforcement agencies. In addition, this service and information is provided to Federal, state and local international law enforcement agencies to assist them in building investigations, preparing prosecutions, and developing and facilitating strategies to counteract criminal activities related money laundering.

FinCEN has identified tactful strategies that help to facilitate the processing of anti-money laundering programs, they include:

- Working with law enforcement, regulatory, and financial institutions as a partnership to combat money laundering.
- Focus on global attention and increasing international awareness of the impact of money laundering (e.g., Financial Intelligence Units).
- Understanding the role of innovative technology and developing systems to combat money laundering.

In the June 2010 (Issue 14) report by FinCEN that covers the SAR Activity Review (by the Numbers) illustrates the following money laundering SAR filings by financial institutions: ²¹

- **U.S. Depository Institutions** filed 2.6 million money laundering SARs and represents an estimate of 0.78 percent to 4.7 percent of global money laundering transactions.

²⁰ "IMF - Anti-Money Laundering/Combating the Financing of Terrorism - Reference Materials and Model Laws," *Vienna Convention in 1988*, November 2010, <http://www.imf.org/external/np/leg/amlcft/eng/aml4.htm>.

²¹ "FinCEN - SAR Activity Review - By the Numbers," *Issue 14 - June 2010*, November 2010, http://www.fincen.gov/news_room/rp/sar_by_number.html.

- **U.S. Casino’s and Card Clubs** filed 2,775 money laundering SARs and represents an estimate of 0.0008 percent to 0.005 percent of global money laundering transactions.
- **U.S. Securities and Futures** filed 18,313 money laundering SARs and represents an estimate of 0.0055 percent to 0.033 percent of global money laundering transactions.
- **U.S. Money Service Businesses** filed 0.00 money laundering SARs which implies that they are not complying with AML/CFT regulations and requires investigation.
- **U.S. Insurance** filed 0.00 money laundering SARs which implies that they are not complying with AML/CFT regulations and requires investigation.
- **U.S. Precious Metals/Jewelry** filed 0.00 money laundering SARs which implies that they are not complying with AML/CFT regulations and requires investigation.

After FinCEN has received SAR filings, multiple Federal agencies may be called upon for further investigation of the money laundering violations. FinCEN’s top five agencies namely, (1) the Drug Enforcement Agency (DEA), (2) the Federal Bureau of Investigation (FBI), (3) the U.S. Secret Service, (4) the Internal Revenue Service’s Criminal Investigation, and (5) the U.S. Customs Services Immigration and Customs Enforcement:

I. U.S. Department of Justice

(1) Drug Enforcement Agency (DEA) – the DEA is called upon to investigate illicit drug proceeds that are managed as a **smuggled goods** investigation, in contrast to the more the traditional money laundering investigation of **asset tracing**. The DEA has identified the following money laundering threats:²²

- *Bulk currency smuggling;*
- *Currency exchange houses; and*
- *Remission of drug proceeds through U.S. based money remitters.*

²² “Inside the DEA, DEA Programs, Money Laundering,” November 2010, <http://www.justice.gov/dea/programs/money.htm>.

DEA news on money laundering and drug contraband charges:

- http://www.justice.gov/dea/pubs/pressrel/moneylaunder_index.html ²³

(2) Federal Bureau of Investigation (FBI) – the FBI investigates the asset tracing of illicit proceeds and uses FinCEN’s financial database known as, BSA data to investigate and prosecute suspects of money laundering.²⁴

BSA data source is based at FinCEN of the U.S. Department of Treasury – there is no public resource to determine the private data that is stored but may include data sources such as, (a) Law enforcement information, (b) Company databases, (c) Nominee and beneficial ownership information (trusts, IBCs...), (d) Financial information other than from the reporting institution, (e) Public information, (f) Population register, (g) Vehicle registration, (h) Land register, (i) Internet and Social Networking Links, (j) Customs, (k) Internal Revenue Service, (l) Social Security / Welfare, (m) Interpol, (n) Egmont Group Financial Intelligence Units (FIU), (o) the United Nations Office on Drugs and Crimes, and many other data sources.²⁵

II. U.S. Department of Homeland Security

(3) U.S. Secret Service – *is responsible for maintaining the integrity of the nation’s financial infrastructure and payment systems. As a part of this mission, the Secret Service constantly implements and evaluates prevention and response measures to guard against electronic crimes as well as other computer related fraud. The Secret Service derives its authority to investigate specified criminal violations from Title 18 of the United States Code, Section 3056.*

The Money Laundering Control Act makes it a crime to launder proceeds of certain criminal offenses, called "specified unlawful activities," which are defined in Title 18, United States Code, Sections 1956 & 1957; as well as Title 18, United States Code, Section 1961 (Racketeer Influenced and Corrupt Organizations Act). The Secret Service monitors money laundering activities through other financial crimes such as financial institution fraud, access device fraud, food stamp fraud and counterfeiting of U.S. currency.²⁶

III. U.S. Department of Treasury

(4) Internal Revenue Service’s Criminal Investigation – *is the law enforcement arm of the IRS that has global staff that investigates and assists in the prosecution of complex financial*

²³ “News from DEA, Money Laundering News Releases,” November 2010, http://www.justice.gov/dea/pubs/pressrel/moneylaunder_index.html.

²⁴ “FBI — Dismantling Global Money Laundering Operations,” November 2010, <http://www.fbi.gov/news/testimony/dismantling-global-money-laundering-operations>.

²⁵ “FinCEN - BSA Data,” November 2010, http://www.fincen.gov/statutes_regs/bsa/bsa_data.html.

²⁶ “United States Secret Service: Criminal Investigations,” November 2010, <http://www.secretservice.gov/criminal.shtml>.

*crimes related to tax evasion, money laundering, organized crime and narcotics trafficking related to financial crimes, public corruption, and much more.*²⁷

Table 1 - IRS Money Laundering Investigations²⁸

Money Laundering Investigations	FY 2010	FY 2009	FY 2008
Investigations Initiated	1597	1341	1422
Prosecution Recommendations	1240	1048	1305
Indictments	1066	936	1200
Sentenced	751	753	686
Incarceration Rate	83.8%	85.9%	84.7%
Average Months to Serve	69	72	67

Source: Internal Revenue Service (IRS) – Statistical Data - Money Laundering

(5) U.S. Customs Services Immigration and Customs Enforcement – *customs is the nation’s principal border agency, ensuring that goods entering and exiting the U.S. do so in accordance with U.S. laws and regulations. Custom’s law enforcement activities include interdicting illegal narcotics, child pornography, and other contraband and preventing the importation of hazardous substances into the United States.*

8. AML – Prosecution

Referencing Table 1 – U.S. Money Laundering and SAR Analysis, having SAR reports for money laundering is helpful for evaluating the outcomes of further investigation and prosecution for money laundering offenses. After careful analysis, there is an assumption that 1.433 percent of the total number of filed SARs per year will result in suspects being charged and/or convicted of a money laundering financial crime. The data sources used for the analysis have come from FinCENs Suspicious Activity Reporting by the Numbers (Issue 14, June 201),²⁹ the Organization of Economic Cooperative Development (OECD) National Accounts of Gross Domestic Product (GDP),³⁰ and the Bureau of Justice Statistics (BJS).

The scale of money laundering is somewhat perplexing because the estimates of money laundering vary depending on the given source. *“The International Monetary Fund (IMF) estimates that between 2 to 5 percent of the world’s Gross Domestic Product (GDP) or \$500 billion to \$1.5 trillion is laundered every year through the global financial system where the U.S. government estimates the amount to be \$3.0*

²⁷ “IRS - Criminal Enforcement,” November 2010, <http://www.irs.gov/compliance/enforcement/article/0,,id=98205,00.html>.

²⁸ “IRS - Statistical Data - Money Laundering,” n.d., <http://www.irs.gov/compliance/enforcement/article/0,,id=113002,00.html>.

²⁹ “FinCEN - SAR Activity Review - By the Numbers (Issue 14, June 2010),” November 2010, http://www.fincen.gov/news_room/rp/sar_by_number.html.

³⁰ “OECD Statistics (GDP),” November 2010, <http://stats.oecd.org/index.aspx>.

*trillion, thus, equating to a large number of illicit cash transactions at a financial institution.”*³¹ Assuming that the transactions are less than \$10,000 -- to avoid Cash Transaction Reporting (CTR) – then the number of cash transactions can possibly range from 55 million to 333 million money laundering transactions.

The Bureau of Justice of Statistics (BJS) reported that during the year of 2001, *“FinCEN reported 109,008 Money Laundering SARs where 1,573 defendants were charged in U.S. district courts with money laundering offenses. These defendants comprised 1.8 percent of all cases filed. Of the cases concluded in 2001, 1,243 defendants were convicted of a money laundering offense. Federal defendants sentenced for money laundering in 2001 were convicted of laundering amounts ranging from \$2,000 to more than \$100 million. About 20 percent of the cases involved over \$1.0 million.”*³²

For 2009, FinCEN reported 380,917 filings of Money Laundering SARs where it is estimated that 5,497 suspects will be charged with a money laundering offense. It is underdetermined what the conviction rate will be, but the total amount of money laundered is estimated to range from \$142.6 billion to \$356.5 billion related to the filed cases (ref. Table 1).

Offenders convicted of money laundering face prison terms of up to 20 years, fines up to \$500,000 or twice the value of the property involved, and possible criminal and civil forfeiture related to the value of the property or funds involved.

9. AML – Conclusion

Although AML/CFT efforts are being enforced from protection to prosecution, there are still many weaknesses within the financial institutions that make them vulnerable to money laundering. Given the estimates that 2 to 5 percent of a countries GDP is subject to money laundering is likely. Although, many nations want to control money laundering, they can only accomplish this by removing the lack of AML/CFT resources. For this reason, U.S. law enforcement agencies are prosecuting and convicting a very low percentage (1.4%, 2001 SAR) of SAR suspects and financial institutions have low probability (0.03%, 2009 SAR) of filing a money laundering SAR report (ref. Table 1).

The examination and evaluation of this data defines a single conclusion – that is, AML/CFT programs and law enforcement is highly inefficient and it is mostly likely attributable to the lack of AML/CFT resources.

³¹ Stephen Stead, “Anti money laundering - compliance vs. detection,” November 2010, <http://www.creditcontrol.co.uk/features/legalaspects/00002.htm>.

³² Mark Motivans, “Bureau of Justice Statistics (BJS) - Money Laundering Offenders, 1994-2001,” November 2010, <http://bjs.ojp.usdoj.gov/index.cfm?ty=pbdetail&iid=790>.

Table 1 – Money Laundering Analysis

U.S. Suspicious Activity Reports (SAR)		BSA, Structuring, Money Laundering (ML) SARs											
FinCEN Actual Data	Form	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	
Depository Institutions	SAR-MSB		90,606	108,925	154,000	155,468	214,797	303,318	302,818	347,398	382,338	376,718	
Money Services Business	TD F 90-22.47		-	-	-	-	-	-	-	-	-	-	
Casinos & Card Clubs	SAR-C		36	83	79	217	295	324	277	373	431	523	
Securities & Futures Industries	SAR-SF		-	-	-	1,083	1,462	1,773	2,288	3,994	4,037	3,676	
FinCEN - Total Number of ML SARs			90,606	90,642	109,008	154,079	156,768	216,554	305,415	305,383	351,765	386,806	380,917
BJS - ML Prosecutions (a=act., e=est.)	1.443%	1,854(a)	1,591(a)	1,573(a)	2,223(e)	2,262(e)	3,125(e)	4,407(e)	4,407(e)	5,076(e)	5,582(e)	5,497(e)	
Average of SARs	231,631												
Standard Deviation of ML SARs	117,614												
Change of ML SARs (%)		--	0%	18%	35%	2%	32%	34%	0%	14%	9%	-2%	
Average ML SARs (%)	14%												
Standard Deviation of ML SARs (%)	15%												
Probability of ML SAR being filed		0.39%	0.39%	0.33%	0.22%	0.22%	0.13%	0.06%	0.06%	0.04%	0.03%	0.03%	

OECD - U.S. GDP, million		8,526,200	9,898,800	10,233,900	10,590,200	11,089,200	11,812,300	12,579,700	13,336,200	13,995,000	14,296,900	14,043,900
ML of U.S. GDP (\$), est. Lower	2.0%	170,524	197,976	204,678	211,804	221,784	236,246	251,594	266,724	279,900	285,938	280,878
ML of U.S. GDP (\$), est. Upper	5.0%	426,310	494,940	511,695	529,510	554,460	590,615	628,985	666,810	699,750	714,845	702,195
Confidence Level, No ML SAR		99.61%	99.61%	99.67%	99.78%	99.78%	99.87%	99.94%	99.94%	99.96%	99.97%	99.97%
Standard Deviation of ML SAR (%)		15%	15%	15%	15%	15%	15%	15%	15%	15%	15%	15%
Confidence Factor (z-score)		2.66	2.66	2.72	2.84	2.85	3.01	3.23	3.23	3.34	3.42	3.41
GDP at Risk of ML (est. Lower), million		67,674	78,572	82,820	89,632	94,096	105,794	121,014	128,288	139,258	145,750	142,600
GDP at Risk of ML (est. Upper), million		169,186	196,430	207,051	224,079	235,239	264,486	302,534	320,719	348,146	364,374	356,499

World Gross Domestic Product (W.GDP)

OECD members - W.GDP, million (i)		24,243,137	27,721,393	28,810,939	29,906,711	31,001,046	32,903,784	34,844,404	37,397,234	39,526,702	40,846,721	40,050,453
U.S. GDP to W.GDP (%)		35.2%	35.7%	35.5%	35.4%	35.8%	35.9%	36.1%	35.7%	35.4%	35.0%	35.1%
Rate of Change (%)		--	1.5%	-0.5%	-0.3%	1.0%	0.4%	0.6%	-1.2%	-0.7%	-1.2%	0.2%
Average Rate of Change	-0.03%											
Standard Deviation	0.9%											

Estimated World Money Laundered, million

Money Laundered (est. Lower W.GDP)	2.0%	484,863	554,428	576,219	598,134	620,021	658,076	696,888	747,945	790,534	816,934	801,009
Money Laundered (est. Upper W.GDP)	5.0%	1,212,157	1,386,070	1,440,547	1,495,336	1,550,052	1,645,189	1,742,220	1,869,862	1,976,335	2,042,336	2,002,523

(i) World GDP includes all Member countries of the OECD except Chile, Israel and Slovenia i.e Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States.