THE USE OF CUSTOMER DUE DILIGENCE TO COMBAT MONEY LAUNDERING

Josetta S. McLaughlin
Walter E. Heller College of Business Administration
Roosevelt University\
1400 N. Roosevelt Boulevard
Schaumburg, IL 60173
jmclaugh@roosevelt.edu

Deborah Pavelka
Walter E. Heller College of Business Administration
Roosevelt University
430 N. Michigan Avenue
Chicago, IL 60605
dpavelka@roosevelt.edu

==========

ABSTRACT

This paper describes the use of customer due diligence (CDD) policy based on the Know Your Customer (KYC) principle and its role in combating money laundering, in particular by banking institutions. The discussion begins with a description of the context within which anti-money laundering (AML) strategy is designed. An AML framework places customer due diligence policy and associated procedures within a risk management function. Relevant U.S. statutes and the US strategy for preventing money laundering using the KYC principle are identified as important components of AML risk management.

INTRODUCTION

On Tuesday, December 11, 2012, *The Wall Street Journal* reported that the UK-based banking company HSBC acknowledged ignoring possible money laundering activities at its USA branch banks (Barrett & Perez, 2012). The admission was made as part of a $1.9 billion settlement with multiple U.S. agencies, including the Justice Department, the Treasury Department, and the Manhattan district attorney. According to *The Wall Street Journal*, "the bank will admit to violating the (U.S.) Bank Secrecy Act, the Trading with the Enemy Act and other U.S. laws intended to prohibit money laundering…" (Barrett & Perez, 2012). This paper builds on such evidence of fraudulent banking activities by focusing on the context of money-laundering detection and prevention in the banking industry. We examine this context through describing implementation of customer due diligence policies based on the Know Your Customer (KYC) principle.

The paper is organized as follows. First, background information is introduced to set the context in which the Know Your Customer (KYC) principle is applied, including defining the role of customer due diligence initiatives in combating money laundering. The Anti-money Laundering (AML) Regime is then introduced, and the placement of customer due diligence (CDD) initiatives based on the KYC principle within the regime is described. This is followed by identification of statues and mandates that drive AML strategy. CDD policies and procedures are then interpreted relative to the risk management function and AML effectiveness.

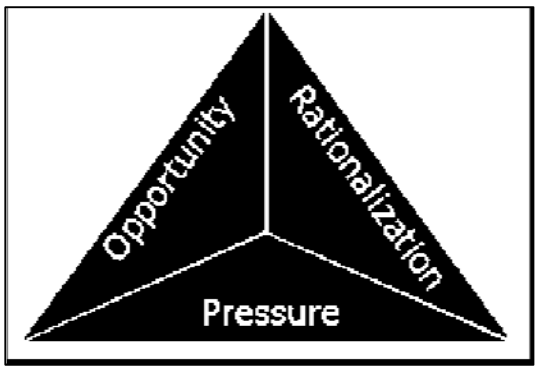
BACKGROUND

There are multiple methodologies used by money launderers to move ill-begotten money into legitimate institutions. An example -- often manifested by money launderers -- is the movement of money into financial institutions through the use of multiple cash deposits, checks, credit cards, investment products, insurance and wire transfers. Such practices place financial institutions at risk of unknowingly becoming complicit in a money laundering action. To manage this risk, U. S. institutions have incorporated customer due diligence (CDD) guidelines based on the Know Your Customer (KYC) principle as part of their anti-money laundering (AML) strategies. These CDD policies require that financial institutions identify and verify the identity of customers on the basis of the information obtained from reliable sources. The responsibility for identifying customers has been complicated by the difficulties inherent in identifying beneficial owners (i.e., “the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted” (Glossary, n.d.)). The definition for beneficial owner may be applied to beneficiaries under insurance policies and to ownership or control that is exercised through a “chain of ownership or by means of control other than direct control” (Glossary, n.d.).

The CDD policies and procedures implemented under the KYC principle are required of all firms operating in the U.S. that are covered under the Bank Secrecy Act of 1970 (BSA), a major piece of federal legislation that specifies the conditions for coverage.

Similar mandates exist in most countries which require that CDD rules be developed and implemented as one part of their AML initiative. Globally, the goal is to prevent money-laundering activities by creating internal controls that mitigate the three components of the Fraud Triangle (Figure 1). The triangle identifies circumstances that open the door for fraud (i.e., the opportunity to commit fraud, the rationalization for fraudulent activities, and the motivation that creates pressures to act fraudulently; for additional information, see Cressey, 1953).

FIGURE 1: THE FRAUD TRIANGLE



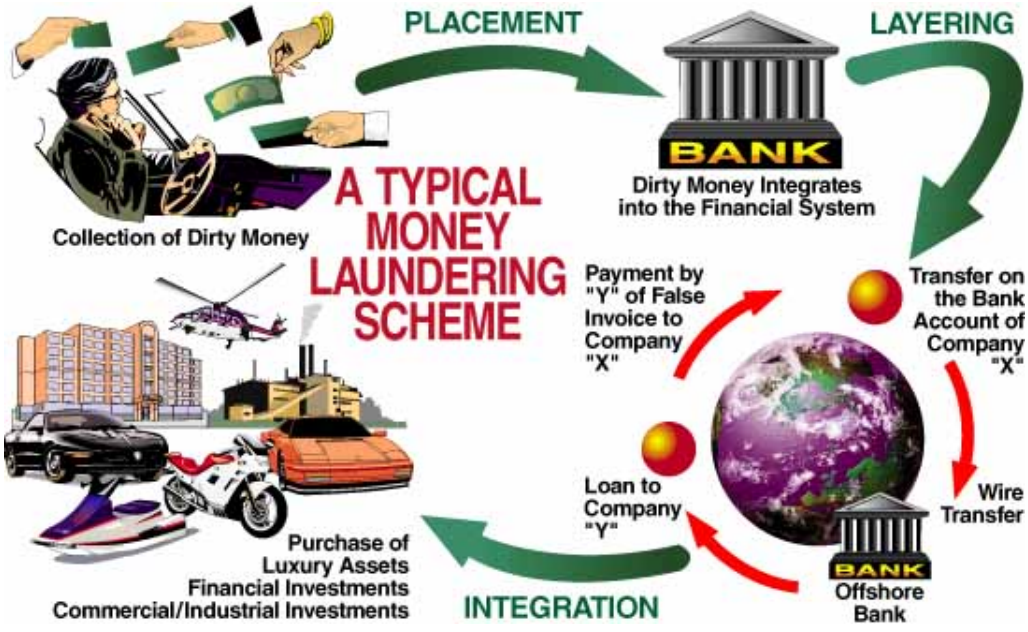
Source. http://www.usi.edu/internalaudit/fraud.asp

Money-laundering (ML) is but one of many forms of fraud. It refers to "(t)he conversion or transfer of property derived from a criminal offence for the purpose of concealing, or disguising, the illicit origin of the money" (Banker's glossary, 2009). The exact monetary cost associated with this type of global criminal activity is unknown but is estimated to range from $600 billion USD to $2.8 trillion USD annually (KPMG International, 2007; OCC, 2002, Dec.). The scope of industries being exploited by money launderers is becoming increasingly broad and includes real estate, casinos, and other industries through which large amounts of money are moved. Historically, financial institutions, including traditional banks and non-bank money service entities, have been especially visible and vulnerable to exploitation.

Understanding money laundering schemes is important to creating internal controls to prevent these practices. As shown in Figure 2, the schemes generally follow three linear phases – Placement, Layering, and Integration (Layton, n.d.; OCC, 2002, Dec.).

During the Placement phase, the customer inserts dirty money into a legitimate business organization using common instruments such as the cash bank deposit. The second phase, Layering, refers to the process of breaking the money into smaller amounts and moving the smaller money amounts through multiple financial transactions, often crossing country borders and forms, making the monies more difficult to trace. The different tactics used to move money are broad, from "bank-to-bank transfers, wire transfers between different accounts in different names in different countries, manipulating accounts through ongoing deposits and withdrawals, currency exchanges, and purchase of luxury items (Layton, n.d.; McLaughlin, Pavelka, & Amoroso, 2010; OCC, 2002, Dec.). The final phase, Integration, refers to movement of the monies back into the mainstream economy in a manner that creates an illusion of legitimacy by making the transaction appear to be legal. Tactics range from purchase of products at exorbitant prices, sham purchases, transfers into the account of a local business to an investment in exchange for a cut of the profits (Layton, n.d.; McLaughlin, Pavelka, & Amoroso, 2010; OCC, 2002, Dec.).

FIGURE 2: PHASES OF MONEY LAUNDERING



Source: International Money Laundering Information Network. Retrieved from www.imolin.org/images/imolin/schemeng.jpg

Policies and procedures based on the KYC principle are most effective in preventing ML activities if applied during the Placement phase. Geister (2008) notes that implementation of associated CDD procedures is the most effective means for guarding against ML activities and other financial crimes. This is true for a number of reasons. First, ML activities are by nature clandestine and discriminating, making those institutions with weak or ineffective internal CDD controls especially vulnerable to exploitation and to becoming unintentionally involved in illicit activities. If financial institutions are not positioned to recognize and prevent clandestine activities at their onset, the likelihood of detecting ML schemes decreases as you progress through each of the three phases. Failure during the Placement phase thus significantly increases the likelihood that the launderer will never be apprehended. Second, lack of a sophisticated CDD strategy represents a failure of the financial institution to recognize the increasingly complex and dynamic environment in which it operates. Money launderers have historically inserted dirty money into legitimate institutions using common instruments such as the cash bank deposit; today other less obvious mechanisms such as loaded credit cards are increasingly used to avoid detection. This is due, at least in part, to heightened enforcement and requirements that financial institutions report large monetary transactions and that beneficial owners be identified (McLaughlin, Pavelka, & Amoroso, 2010). Frameworks for supporting AML compliance have also been developed.

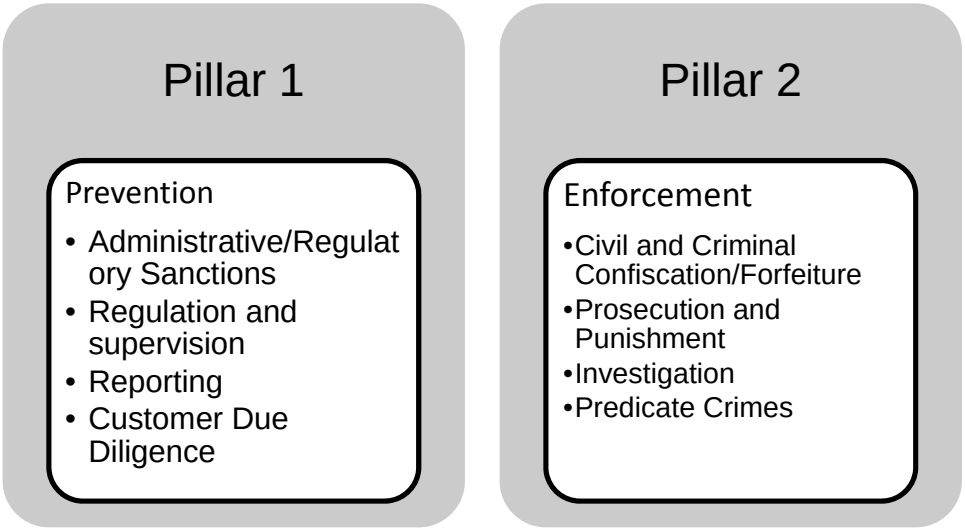
THE AML REGIME

The most frequently cited AML compliance scheme is the Reuter/Truman AML Regime (Reuter & Truman, 2004). The model, shown in Figure 3, has two components or pillars -- Prevention and Enforcement (Levi & Reuter, 2006, p. 298). Elements under the Prevention Pillar are intended to create sufficient transparency to deter criminals from using legitimate organizations to launder proceeds; elements under the Enforcement Pillar are intended to punish criminals and their associates for ML activities.

Customer Due Diligence (CDD) is found at the base of the Prevention Pillar (Levy & Reuter, 2006, p. 297). The “Know Your Customer” policies that define CDD form the

foundation for Prevention. They are, as noted previously, intended to deter access to financial institutions by customers that benefit from crime or terrorist financing. CDD guidelines require that covered institutions collect identifying data on account holders or the beneficiary (i.e., beneficial owners) on whose behalf the holder is acting, proof of the customer's identity and information concerning their circumstances (Levy & Reuter, 2006, p. 297). This will be discussed in more detail later in the paper. These procedures are intended to prevent money lauders from gaining access to legitimate institutions. The remaining elements of the pillar are Reporting, Regulation and Supervision, and Sanctions to be imposed where appropriate (Levy & Reuter, 2006, p. 297; McLaughlin, Pavelka, & Amoroso, 2010).

FIGURE 3: THE AML REGIME



Source: Reuter & Truman, 2004

Identification of predicate crimes, an offence that generates proceeds that may become the subject of an action, is at the base of the Enforcement Pillar. Once the process has reached this Pillar, law enforcement agencies, not the financial institutions, determine the outcome. As noted in Exhibit 1, predicate crimes establish a legal basis for criminalizing ML (Levy & Reuter, 2006, p. 299; OCC, 2002, Sept.). Investigation, prosecution and criminal confiscation or forfeiture can only be implemented if predicate crimes can be identified. The list of possible predicate crimes is voluminous -- ranging

from human trafficking, gunrunning, murder for hire, fraud, and acts of terrorism to the illegal use of wetlands, white collar crimes, and certain foreign crimes (OCC, 2002, Sept.). The other elements of Pillar 2 are Investigation, Prosecution and Punishment, and Civil and Criminal Confiscation/Forfeiture (Levy & Reuter, 2006, p. 299).

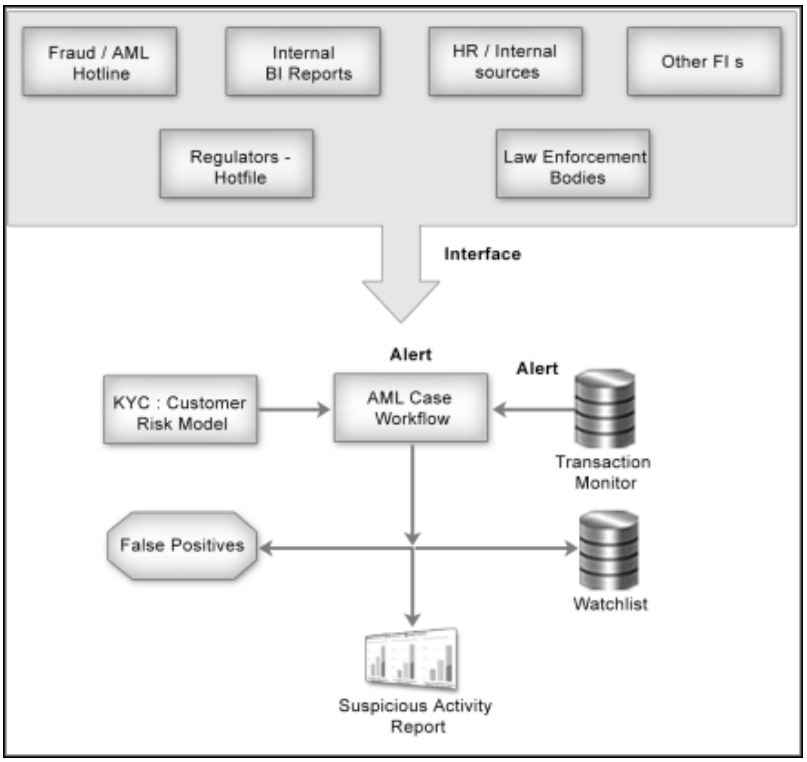
EXHIBIT 1: PREDICATE OFFENCE

Understanding how money laundering fits within the larger classification of corruption activities requires understanding of the "predicate offence." For purposes of money laundering, a "predicate offence" is an offence that generates proceeds that may become the subject of an action listed in the various corruption conventions. For example, The UN Convention Against Corruption, Article 2(h), states that "(f)or the purposes of this Convention, 'predicate offence' shall mean any offence as a result of which proceeds have been generated that may become the subject of an offence as defined in article 23 of this Convention" (OECD, 2007). Article 23 identifies as a predicate offence "(t)he conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action" and "(t)he concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime" (OECD, 2007). Because corruption is by definition a crime intended to secure ill-gotten proceeds, most forms of corruption can be treated as a "predicate offence."

Source: McLaughlin, Pavelka, & Amoroso, 2010

The Reuter/Truman AML Regime provides a pictorial guide for financial institutions in developing and implementing an overall approach to AML strategy. Other useful frameworks position CDD initiatives (known frequently only as KYC programs) as an element within a broadly-based enterprise risk management function. Enterprise risk management strategies are intended to address the institution's overall exposure to a multitude of external and internal threats (Business Glossary, n.d.) while KYC programs target a specific threat. As suggested by Figure 2, the KYC program ultimately leads to filing of reports about suspicious activities; these reports are generally referred to as "suspicious activity reports" or SARS.

FIGURE 4: RISK MANAGEMENT FLOW CHART



Source: http://cdn.information-management.com/media/assets/article/1093412/10.2%20natarajan_fig1.gif

In the U.S., implementation of risk-based procedures and filing of SARS are required by agencies of the Department of the Treasury. Financial institutions must "establish and implement risk-based procedures for verifying the identity of each customer" and must file suspicious activity reports (SARs) with enforcement agencies when criminal violations are suspected (About the OIG, 2009). The goal is for a financial institution to define and implement a set of policies and procedures to ensure that it is complying with AML and terrorist financing (TF) requirements, in particular, those specified in the Bank Secrecy Act of 1970 (BSA). A number of rating systems have been developed for this purpose. For example, the international bank-rating system known as the CAMELS Rating System examines six factors: Capital Adequacy, Asset Quality, Management Quality, Earnings, Liquidity, and Sensitivity to Market Risk (CAMELS Rating System, n.d.). Each factor is scored on a scale of one (best) to five (worst). Banks with average scores of less than two are considered to be high-quality. Similar to the CAMELS

Rating System is the ROCA rating system for federal branches and agencies. It rates four areas: Risk Management, Operational Controls, Compliance and Asset Quality (OCC, n.d.). Risk management is given the highest priority. This is true both in the U.S. and under global AML standards, including those established under the U.S. Patriot Act (2001), the Basel Committee on Banking Supervision (Kentouris, 2010) , and the Financial Action Task Force (FATF-GAFI, n.d.).

CUSTOMER DUE DILIGENCE PROGRAMS

In the U.S., national legislation dictates that risk management processes be articulated when implementing customer due diligence programs using the KYC principle. At another level beyond the U.S., legislation and mandates must be consistent with a vast global infrastructure designed to address global ML problems (BIS, n.d.; FATF-GAFI, n.d.). Programs implemented under the KYC principle are thus similar from country to country. Debra Geister (n.d.) describes the generic processes used in customer due diligence:

> CDD begins at account opening and the determination of the level of AML risk that your customer poses to the institution is a fundamental part of this process. The first step in efficient CDD is getting as much information as possible at the beginning of the institution's relationship with the customer. Having a customer identification program (CIP) that includes thorough information gathering and verification procedures is essential for assuring that you have enough data to assign an accurate level of risk to your new customer. Not having enough information or having inaccuracies in the information that is collected is likely to create a "domino effect" that may lead to your institution being used to launder funds and a subsequent regulatory or criminal penalty. In addition to having a risk-based approach it is expected that the entity has a CIP verifying customer data done both through physical documents or nondocumentary methods. Physical document include the collection of a driver's license, passport, or other government-issued identification. Nondocumentary methods include speaking to the customer, consumer credit-reporting agencies, the internet, other financial institutions, and publicly available databases.

In the U.S., any entity that cashes or provides monetary instruments[1] exceeding $1,000 falls under the BSA and must therefore establish, maintain, and provide necessary

[1] Monetary instruments are defined to include money orders, traveler's checks, electronic or other forms of money transmission, check cashing, currency exchange, currency dealing, and stored value cards.

reporting required under KYC policy. This is strengthened by Section 326 of the Patriot Act of 2001 which requires that a customer identification programs (CIP) is in place when new accounts are opened (FDIC's Implementation of the USA PATRIOT Act, 2007). Section 326 also requires that the CIP procedures be capable of determining whether individuals opening the account appear on lists of known or suspected terrorist or terrorist activities. Common information required for a customer opening an account or doing a transaction include customer's identity; nature of business activity, location of customer, mode of payments, volume of turnover, public or high financial status, product type, source of funds, transaction type, transaction value, type of entity, and any other matter that a bank may find fit to consider (McLaughlin, Pavelka, & Amoroso, 2010).

The Suspicious Activity Report (SARs) -- also referred to in some countries as a Suspicious Transaction Report (STR) -- is the primary vehicle for compliance with national and global standards. SARs are submitted to the country's specified agency; the agency then analyzes and investigates those activities identified by the institutions as abnormal or unexpected in nature. These reporting structures increasingly use the newest and most innovative tools to monitor activities which include the World Wide Web, data warehousing and graphical user interface software. The tools enable financial institutions to incorporate data mining both internally within the institution and across different types of institutions, thus enabling cross-border communication among the appropriate enforcement agencies to be more efficient and effective (Watkins, et al., 2003). Software companies respond by developing products that enable a financial institution to provide comprehensive lifecycle management of customer data from the initial point of collection to verification of customer identity and assessment of a customer's risk, all in real time (see, for example, http://www.actimize.com/).

U.S. STATUTES AND SUPPORTING MANDATES

The processes described above are supported in the U.S. by laws and their associated regulations. For example, implementation of KYC programs (i.e., CDD policies and procedures) by U.S. financial institutions is mandated by The Financial Recordkeeping

and Reporting of Currency and Foreign Transactions Act of 1970 (31 U.S.C. 1051 et seq.), referred to earlier by its common name --The Bank Secrecy Act of 1970 (BSA). In conjunction with Title III of the USA Patriot Act of 2001, the BSA forms the pillars for regulation and enforcement of U.S. AML initiatives (Levi & Reuter, 2006). More importantly, it authorizes the U. S. Treasury Department to establish reporting standards for financial institutions. In 1990, the U.S. Treasury created the Financial Crimes Enforcement Network (FinCEN) as its enforcement arm for "facilitating the detection and deterrence of financial crime" (FinCEN, n.d.). Title III of the USA Patriot Act further expanded the BSA's scope to better address problems associated with criminals using banks by establishing new standards for records access and minimum standards for customer identification. It also broadened its scope by addressing problems associated with some non-bank financial service providers. Such providers, sometimes referred to as shadow banks, are financial intermediaries that " conduct maturity, credit, and liquidity transformation without explicit access to central bank liquidity or public sector credit guarantees" (Pozar, et al.,2010). Regulatory requirements were thus broadened to cover an ever growing variety of institutions under BSA, including many non-banking institutions that could be arguably involved in financial and financial-related transactions. Subsequent legislative modifications also brought pending bank mergers, acquisitions and other business combinations under scrutiny for potential suspicious activity (USA PATRIOT Act, 2001). A vast network of language from other legislation and associated regulations further support AML activities by financial institutions.

Responsibility for BSA is shared by more than 12 U.S. government agencies (Audit Report, 2008). There is also a dedicated national strategy for combating ML that is updated on a regular basis. The current U.S. strategy for combating ML was published in 2007 in response to the publication of the 2005 U.S. Money Laundering Threat Assessment (*2007 National Money Laundering Strategy*, 2007). The U.S. 2005 threat assessment revealed that the most vulnerable institutions continue to be banks; however, money services businesses, also known as alternative remittance systems, offer an efficient and low cost alternative to banks for both financial services and money laundering. The assessment also revealed that criminals had created a well-

established, ML methodology, especially with respect to use of international trade for disguising transfer of funds. In response to these threats, the U. S. committed to supporting global AML capacity building and enforcement efforts (*2007 National Money Laundering Strategy,* 2007).

Recent attempts by the U.S. Congress to pass new AML laws have focused primarily on specific problems -- for example, the problem of beneficial ownership. Though unsuccessful in being passed as of the beginning of 2013, the U.S. Senate legislation (S. 1483) version of the Incorporation Transparency and Law Enforcement Assistance Act would require stricter standards for defining, filing, and verifying beneficial ownership information with a state at the time of business formation and for all annual filings. The bill defines beneficial owners using Financial Action Task Force (FATF) language which is "a natural person who, directly or indirectly exercises substantial control over a corporation or limited liability company; or has a substantial interest in or receives substantial economic benefits from the assets of a corporation or limited liability company" (NASS, 2012, p. 8). The U.S. House version of the bill (H.R. 3416) uses a different definition of beneficial owner: "natural person who directly or indirectly has at least as great an ownership interest in the corporation or limited liability company as any other natural person, or has responsibility for directing the regular operations of the corporation or limited liability company" (NASS, 2012, p. 10). Due to state concerns regarding this legislation, including its potential impact on the U.S. business formation process, its costs and its compliance burdens, critics believe that the U.S. is unlikely to pass these or similar AML bills into law (NASS, 2012).

SUPPORTING AML INITIATIVES

Implementation of AML initiatives and mandates at the nation state level is feasible due to the global infrastructure that has evolved to support prevention and enforcement efforts. At the global level, two previously identified organizations, – the Basel Committee on Banking and the Financial Action Task Force (FATF), fill a critical role by developing and publishing relevant research, guidance documents, and reports. The Basel Committee on Banking is a committee of the Bank for International Settlements,

an organization that focuses primarily on matters related to banking supervisory. The Committee's stated objective is "to enhance understanding of key supervisory issues and improve the quality of banking supervision worldwide" (About the Basel Committee, n.d.). In its effort to promote common understanding among financial institutions, the Basel Committee has published -- and made available for free -- thousands of papers designed to guide banks in setting up customer due diligence systems. For example, the document "Customer Due Diligence for Banks" was published in October 2001 to address issues that are associated with adequacy of controls and procedures that enable a bank to know the customers with whom it is dealing. In 2003, the Committee published "Consolidated KYC Risk Management" as a supplement to its 2001 paper to identify, among other things, "the critical elements for effective management of KYC policies and procedures" (Consolidated KYC Risk Management, 2003).

The Financial Action Task Force (FATF) was created during the 1989 Paris G-7 Summit as an independent policy-making intergovernmental body. Its initial charge was to develop and promote "national and international policies to combat money laundering and terrorist financing" (About the FATF, n.d.). Consistent with this charge, the FATF now conducts research on money laundering techniques and trends, reviews national and international actions, and identifies measures for assessing ML activity (McLaughlin, Pavelka, & Amoroso, 2010). Research efforts include studies of ML trends in various industry sectors, studies of non-cooperative countries and territories, and assessment of regional and sector compliance with FATF standards. The FATF regularly publishes resources to support implementation of AML systems for industry sectors and professionals (FATF-GAFI, n.d.).

FATF publications provide authoritative information on interpretation of its 12 *Strategic Issues* and 40 *Recommendations*[2] for combating ML (About the FATF, n.d.). With respect to customer due diligence, FATF Recommendations state that financial

[2] FATF's *40 Recommendations,* originally adopted in 1990, updated in 1996 and again in 2003, provide counter-measures against ML. They were expanded with 9 special recommendations following September 11, 2001, to criminalize terrorist financing and laundering of money associated with terrorism. (9 Special Recommendations, n.d.; The 40 Recommendations, 2003).

institutions should be required by law or regulation "to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions" (FATF, Recommendation 10). FATF also recommends that identification requirements should include verifying that a person claiming to act on behalf of a customer is authorized to do so. FATF thus recommends the processes for customer identification and identifies standards for record keeping that are intended to create an effective infrastructure for AML initiatives.

Scholarly and practitioner publications provide some guidance on implementation of AML initiatives. Interestingly, very little of the scholarly literature exists in U.S. journals of business that explore topics related to AML, including the effectiveness of customer due diligence programs. Most scholarly articles focus on broader ML topics and are found in journals that specialize in topics related to criminology[3]; a few are found in legal journals.[4] In contrast, a large body of articles in the practitioner literature exists to advise financial institutions on how to create an infrastructure for effectively implementing customer due diligence initiatives based on KYC principles. Practitioner articles are designed to meet the present needs of financial institutions.[5] The articles are frequently written by consultants and industry experts that have a global perspective and that have access to information that can be used to quickly update the reader on new or pending rules and regulations, on compliance issues, and on applicable AML techniques. Similarly, the information provided by government and quasi-governmental organizations is voluminous and ranges from whitepapers to guidance documents to research. The reliance on practitioner and government or quasi-governmental sources for information is expected, especially given the fact that problems experienced by financial institutions in implementation of CDD/KYC programs require immediate

[3] See, for example, the *Journal of Banking Regulation, Journal of Money Laundering Control, Journal of Investment Compliance,* and *Journal of Financial Crime*.
[4]See, for example, the *European Journal of Law Reform* and *Butterworths Journal of International Banking and Financial Law.*
[5] See, for example, the *Community Banker, ABA Banking Journal, CPA Journal, ACAMS Today*, and *United States Banker.*

assistance. Furthermore the problems that crop up as a result of ML activities are in a constant state of change. As a result, institutions vulnerable to ML problems need assistance in real time for managing the potential risks.

In the USA, authoritative information regarding CDD/KYC provisions of the BSA is available through many of the agencies located within the U.S. Department of the Treasury, one of which is the Office of Inspector General (OIG). Established in 1989, the Office provides the Secretary of the Treasury with "independent and objective reviews of the department's operations" (About the OIG, n.d.). The Inspector General meets this charge through research and production of papers and reports that inform the Secretary and the Congress about the problems and deficiencies in operations. Among the reports are guidance manuals, documents from and about AML standards established by the FATF, and numerous reports that evaluate the effectiveness of U.S. efforts to implements provisions of the BSA (About the OIG, n.d.).

Agencies of the U.S. Treasury also report on compliance with KYC principles that guide implementation of CDD regulations or mandates issued by global quasi-governmental groups. For example, results from the report "Assessment of Compliance with the Basel Core Principles of Effective Banking Supervision" indicates that U.S. bank supervisors are, for the most part, compliant with the 25 Basel Core Principles[6]. The principles, revised in September 2012 from 25 to 29, evaluate the performance of bank supervisions. The reports states that "(t)he United States has a rigorous supervisory regime, involving audit and attestation requirements, leverage ratios and prompt corrective action mandates, comprehensive and frequent disclosure and reporting requirements, sophisticated modeling capabilities, on-site examinations, and a strong focus on risk-management processes" (Department of the Treasury, 2009).

[6] The Core Principles for Effective Banking Supervision, revised in September 2012, are divided into two parts. "Principles 1 to 13 address supervisory powers, responsibilities and functions, focusing on effective risk-based supervision, and the need for early intervention and timely supervisory actions. Principles 14 to 29 cover supervisory expectations of banks, emphasising the importance of good corporate governance and risk management, as well as compliance with supervisory standards" (BIS, 2012).

ENFORCEMENT EFFORTS

As noted, the development of AML policy and procedures, in addition to being global and supported by risk-management initiatives, is increasingly built on a sophisticated technology infrastructure that supports an effective enforcement system. There is some evidence that the system is working. Though violations continue to plague the financial industry sector, awards are more visible and the amounts that banks are fined for money laundering involvement are becoming substantial. For example, the 2012 money laundering settlements in the U.S. for just three institutions amounted to almost $2.9 billion (See Figure 5). This amount does not include settlements for simultaneous charges brought against the banks for violation of other U.S. statutes, for example, the US PATRIOT ACT. The settlement of $340 million between Standard Chartered (a UK bank doing business in the USA) and New York regulators does not include a second and separate settlement with the Federal Reserve, U.S. Department of Justice, and the District Attorney for New York City in the amount of $327 million for violation of USA sanctions against trade with Iran (Sparshott, 2012; Paletta, Barrett, & Enrich, 2012).

FIGURE 5: LARGEST U.S. MONEY LAUNDERING SETTLEMENTS 2009-2012

Institution	Penalty in US millions	Date
HSBC	1,900	December 2012
ING Bank	619	June 2012
Lloyds TSB Bank	567	December 2009
Credit Suisse	536	December 2009
Royal Bank of Scotland	500	May 2010
Standard Chartered	340	August 2012
Barclays	298	August 2010

Sources: Based on information from Paletta, Barrett, & Enrich; Barrett & Perez, 2012; the U.S. Treasury and Justice Department; Steptoe Johnson LLP; and *The Wall Street Journal*

U.S. money laundering probes on European financial institutions operating in the USA occurred simultaneously with probes of U.S. banks. For example, Lennard (2012) reports that Wachovia (now part of Wells Fargo) was the focus of an investigation by the U.S. Drug Enforcement Administration and others concerning laundering of “billions of

dollars of cartel cash." The bank reached a 2010 settlement of $160 million with the U.S. Justice Department following investigations into "casas de cambio" transactions (Lennard, 2012). This followed incidences involving Bank of New York and fines of more than $38 million in 2005 for transactions involving Russian emigres (O'Brien, 2005). Large settlements reported since 2009 and shown in Figure 6 suggest that, despite development of fairly sophisticated AML infrastructures, U.S. banks do remain vulnerable to access by drug cartels and terrorist groups. Implications for performance of banks operating in the U.S. are serious. For example, stock for Standard Chartered Bank dropped 7% immediately following allegations against the bank became public knowledge, even though payment of the settlement was not likely to over-stress the bank's financial situation (Barrett & Perez, 2012). More importantly, banks being investigated for money laundering are likely be simultaneously investigated for other forms of fraud. JP Morgan Chase has been under scrutiny for both money-laundering and for mortgage fraud involving mortgage-backed securities (Lopez, 2012). The latter investigation recently lead to costs of US $297 million to settle lawsuits. The bank had settled in 2005 with investors for $2 billion over charges of fraud involving WorldCom (Rovella & Baer, 2005).

FIGURE 6: EXAMPLES OF BANKS IMPACTED BY CDD & FRAUD

BANK	HEAD-QUARTERS	NATURE OF CHARGE	YEAR	RESULTS/FINES
Bank of New York	United States	Money Laundering (Russian emigres - movement of over US$7 billion via wires)	2005	US $38 million (Suit by Russia settled for $14 million)
JP Morgan Chase	United States	Mortgage Fraud	2012 2005	US $297 million US $2 billion
HSBC	United Kingdom	Money Laundering (Dealings with Mexico's Money-changing firms ("casas de cambio")	2012	US $1.9 billion
Standard Chartered	United Kingdom	Money Laundering & Violation of Trade US Sanctions (with Iran, Burma, Libya, and Sudan)	2012	US $340 (for ML) US $327 (for Trade Sanctions)

Sources: Barrett & Perez, 2012; Lopez, 2012; O'Brien, 2005; Paletta, Barrett, & Enrich, 2012); Rovella & Baer, 2005; Sparshott, 2012

DISCUSSION

The global infrastructure being developed to curb money laundering are significantly impacting operations in the banking industry through requirements that customer due diligence policies and procedures be implemented. Banks operate in a highly competitive environment that requires considerable expenditures on marketing and promotion to attract customers. Balancing the need to be both competitive with the need to be sensitive to the needs of consumers is complicated. This complexity, coupled with the need for legal compliance, has led to criticism of current AML effectiveness. Critics suggest that the impacts of implementing CDD/ KYC programs can potentially have a negative impact on commercial success (Martin & Taylor, 2004).[7] Critics further argue that customer due diligence policies and procedures put financial institutions in a position where they are "spying" on customers and that this puts the institutions at risk for alienating their customers. The concern is that banks might potentially choose to implement only the minimum standards that are required by CDD/KYC regulations (McCusker, 2005, 2006). Nevertheless, the volatility of the environment in which money is laundered has led policymakers to move forward with adopting new strategies for preventing money laundering activities. This is best demonstrated by the current preference at the policy level to change the context in which AML initiatives are implemented, moving from rules-based approach to risk-based.

The risk-based approach to AML that is advocated by FATF and most governments has required a change in attitudes among many industry personnel towards their functional and occupational responsibilities. The challenge facing the industry is now to reinforce this policy change through implementation of new worker training, professional development programs, and changes in technology. As noted earlier, practitioners and consultants are providing substantial assistance in designing training and professional

[7] Efforts to balance operational needs with legal compliance has been further exacerbated by efforts to correct problems associated with the mortgage branch of banking following the housing collapse.

development programs; software companies are providing substantial assistance by designing data mining tools that support the risk management process.

Though impressive advances have been made, there remains the need to validate the effectiveness of a risk-based approach to customer due diligence. Critics of the risk-based approach suggest that the approach does not do what it is supposed to do for a number of reasons. For example, it "presupposes that risks can in fact be identified, analysed and the consequences measured and acted upon effectively by and within organizations" (McCusker, 2005, 2006). This type of assumption "presupposes a highly developed and current knowledge of the actual and prospective threats to an organization and to the sector in which it resides" (McCusker, 2005, 2006). Despite these criticisms, recent settlements for violation of money-laundering statutes (such as that for HSBC and the involvement of the "casas de cambio" in Mexico) are likely to lead to greater support for use of risk-based management by banks to curb money-laundering, especially when the risk involves movement of money across national borders.

With respect to the implementation of CDD policy and procedures, the expected operational problems persist – interpretation, compliance costs, and scope. First, the interpretation of statutes and clarification of terms will likely continue to be a problem in implementation of policies and procedures. For example, determining who should qualify as a politically exposed person (PEP) is a problem for financial institutions at both the national and international level. PEPs are generically defined as "individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves" (The Forty Recommendations, 2003, June 20). Disagreements concern such issues as whether former political office holders and business executives that continue to exercise influence should be treated as PEPs. Difficulties also occur when identifying local PEPs versus non-local PEPs (Green, 2009). Unfortunately, many third-party data bases used

by financial institutions may not provide information at this level of analysis. Furthermore, a problem is encountered by the institutions that are trying to determine both the definition of PEPs to be applied when the persons identified as PEPs are constantly changing.

Second, the most frequently cited concern about required customer due diligence programs is the costs of compliance (McCusker, 2005, 2006). Costs are associated with technology, training, personnel, and consultants, to name only a few. Computer hardware, computer software and the databases need to be continually updated; personnel need to be retrained to meet the ever-changing needs of financial institutions. In addition, the workload of employees is increased due to the magnitude of reports (SARs) that are likely to be sent to financial investigative units such as the U.S. agency FinCEN. There is speculation as to whether agencies will be swamped with non-significant reports to the detriment of real money-laundering cases (Green, 2009). Practitioner articles are now addressing these concerns, but no definitive scholarly research is currently available that comprehensively examines the status and impact of SARs filings.

Third, the scope of industries covered by AML mandates continues to broaden. New money-laundering tactics have spread beyond the traditional industries to now include (to name only a few) real estate, on-line sales, insurance, and credit instruments that have not traditionally been associated with money-laundering. In response, increased efforts in curbing money laundering are likely to result in new proposed regulations and legislation or fast-tracking of currently proposed legislation. Identification of new industries that are vulnerable to money-laundering will be on-going. For example, the concept of “shadow banking” (i.e., financial intermediaries that facilitate credit across global financial systems but that are not subject to regulatory oversight) is already bringing domestic and global non-regulated instruments such as hedge funds to the attention of government regulators (Investopedia, n.d.). Appropriate oversight of “non-bank” banks (e.g., money exchanges, cash checking services, or retail establishments) is also a subject of on-going discussions, even though they are already covered by AML

statutes. Institutions within this broader range of industries are not always technically "banks" but are clearly involved in financial transactions.

With respect to the scholarly business literature, substantially more research is needed to inform scholars and financial institutions about the impacts of CDD/KYC initiatives on the operations of banks and on the larger economy. Definitive studies are also needed on the effectiveness of CDD policy and procedures for addressing money-laundering problems, including protecting vulnerable industries. Measuring effectiveness by simple counting settlement amounts when banks are found to be guilty of violating U.S. AML statutes fails to provide a holistic picture of events. It doesn't fully describe the beneficial impacts of AML initiatives on the economy, and it doesn't speak to issues surrounding employee training, public education, or the sensitive issues surrounding customer tracking. Without the additional research, it is difficult to identify what information should be included in the business curriculum of colleges and universities for educating the students and business professionals who will ultimately work in financial institutions.

REFERENCE LIST

9 Special Recommendations (SR) on Terrorist Financing (TF). (n.d.). Retrieved May 1, 2009, from *http://www.fatf-gafi.org/document/9/0,3343,en_32250379_32236920_34032073_1_1_1_1,00.html*

2007 National Money Laundering Strategy. (2007). Prepared by an Interagency Working Group: U.S. Department of the Treasury, U.S. Department of Justice, U.S. Department of Homeland Security. Retrieved May 1, 2009, from *http://www.treas.gov/press/releases/docs/nmls.pdf*

About the Basel Committee. (n.d.). Bank for International Settlements. Retrieved December 9, 2009, from *http://www.bis.org/bcbs/*

About the FATF. (n,d,) FATF-GAFI. Retrieved May 1, 2009, from *http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236836_1_1_1_1_1,00.html*

About the OIG. (n.d.). Office of the Inspector General. Department of the Treasury. Retrieved December 15, 2009, *http://www.treas.gov/inspector-general/about.shtml*

Audit Report. (2008, April 9). Terrorist financing/money laundering: Responsibility for Bank Secrecy Act is spread across many organizations. OIG-08-030. Office of Inspector General. Department of the Treasury. Retrieved Jan 9, 2010, from *http://www.treas.gov/inspector-general/audit-reports/2008/oig08030.pdf*

Bank Secrecy Act of 1970, 31 USC 1051et seq. Retrieved December 9, 2009, from *http://www.uhuh.com/laws/31usc1051.htm#Introduction*

Banker's Glossary. (2009). American Banker and SourceMedia, Inc. Retrieved April 15, 2009, from *www.americanbanker.com/glossary.html*

Barrett, D. and Perez, E. (2012, Dec. 11). HSBC to pay record U.S. penalty. *The Wall Street Journal* (U.S. Edition). Retrieved January 5, 2013, from *http://online.wsj.com/article/SB10001424127887324478304578171650887467568.html*

BIS. (2012). Core principles for effective banking supervision. Retrieved December 2012, from http://www.bis.org/publ/bcbs230.htm

BIS. (n.d.) Basel Committee on Banking Supervision. Bank for International Settlements. *http://www.bis.org/bcbs/index.htm*

Business Glossary. (n.d.). Dictionary of Banking Terms. AllBusiness. A D&B Company. Retrieved December 9, 2009, from *http://www.allbusiness.com/glossaries/risk-management/4954201-1.html*

CAMELS Rating System. (n.d.). Investopedia. Retrieved Sept. 15, 2012, from *http://www.investopedia.com/terms/c/camelrating.asp#axzz2ChafJoi0*

Consolidated KYC Risk Management, (2003). Bank for International Settlements. Retrieved December 15, 2009, from *http://www.bis.org/publ/bcbs101.htm*

Cressey, D. R. (1953). Other people's money: A study of the social psychology of embezzlement. New York, NY: Free Press.

Customer due diligence for banks. (2001, Jan.). Bank for International Settlements. Retrieved December 15, 2009, from *http://www.bis.org/publ/*

Department of the Treasury. (2009, July 31). Assessment of compliance with the Basel core principles for effective banking supervision. Retrieved December 9, 2009, from *http://www.treas.gov/offices/international-affairs/standards/FSAP/docs/Banking%20Self-Assessment%207-31-09.pdf*

FATF Recommendation 10. (n.d.). Customer identification and record-keeping rules. World Policies. Retrieved January 10, 2010, from *http://www.worldpolicies.com/english/fatf_identification.html*

FATF-GAFI. (n.d.). Publications. Retrieved January 9, 2010, from *http://www.fatf-gafi.org/pages/0,3417,en_32250379_32237235_1_1_1_1_1,00.html*

FDIC's Implementation of the USA PATRIOT Act (2007, Nov.). Report No. AUD-08-003. Retrieved September 1, 2010, from http://www.fdicoig.gov/reports08/08-003-508.shtml

FinCEN. (n.d.). What we do. Financial Crimes Enforcement Network. Retrieved, May 1, 2009, from *http://www.fincen.gov/about_fincen/wwd/*

Geister, D. (2008). Concepts in customer due diligence: Meeting the challenge of regulatory expectations. *LexisNexis® Risk & Information Analytics Group, p. 2*, Retrieved on October 15, 2009, from *http://www.aba.com/NR/rdonlyres/9B9355AC-FB65-4680-8602-9CCCB99D29AB/55127/ccddwp.pdf*

Glossary of the FATF Recommendations. (n.d.) Financial Action Task Force. Retrieved Sept. 15, 2013, from *http://www.fatf-gafi.org/pages/glossary/*

Green, P. (2009, June-August). Implementation of the Third European AML Directive – Remaining challenges. *ACAMS Today*. 8 (3), p. 30-31.

Investopedia. (n.d.). Dictionary. Retrieved from *http://www.investopedia.com/*

Kentouris, C. (2010). Basil III: Enterprise data and risk management required. Information Management. Retrieved on December 29, 2012, from *http://cdn.information-management.com/news/data_risk_management_Basel-10018723-1.htm*l

KPMG International. (2007). Global anti-money laundering survey. Retrieved April 15, 2009, from *http://us.kpmg.com/microsite/fslibrarydotcom/docs/AML2007FULL.pdf*

Layton, J. (n.d.). How money laundering works. How StuffWorks.com. Retrieved April 15, 2009, from *http://money.howstuffworks.com/money-laundering.htm*.

Leonard, N. (2012, Sept. 17). U.S. banks targeted in money-laundering probe. SALON. Retrieved December 15, 2012, from *http://www.salon.com/2012/09/17/u_s_banks_targeted_in_money_laundering_probe/*

Levi, M. and Reuter, P. (2006). Money laundering. In M. Tonry (Ed.). *Crime and justice: A review of research*. 34: 289-375. Chicago: The University of Chicago Press.

Lopez, L. (2012). JP Morgan will pay $297 million to settle SEC mortgage fraud lawsuits. *Business Insider Clusterstock*. Retrieved February 20, 2013, from *http://www.businessinsider.com/jp-morgan-pay-297-mill-sec-settlement-2012-11*

Martin, G., and Taylor, G. (2004). Preventing money laundering or obstructing business? Financial companies' perspectives on "know your customer" procedures. *The British Journal of Criminology. 44* (4): p. 582-94.

McCusker, R. (2005, Dec. 2006, Jan). Early fall-out of the Third Directive. Legislative Review. *Money Laundering Intelligence*, p.13-15.

McLaughlin, J., Pavelka, D., and Amoroso, L. (2010). Money laundering: Strategic initiatives for preventing a growing menace. In Stachowica-Stanusch, A. (Ed.). *Organizational Immunity to Corruption: Building Theoretical and Research Foundations*. US: Information Age Publishing.

NASS. (2012, Sept.). Report and recommendations on assisting law enforcement in fighting the misuse of corporate entities. National Association of Secretaries of State Company Formation Task Force. report-nass-company-formation-task-force-092112.pdf. Retrieved Dec. 15, 2012, from. *http://www.nass.org/*

O'Brien, T. L. (2005, Nov. 9). Bank settles U.S. inquiry into money laundering. *The New York Times.* Retrieved February 15, 2013 from *http://www.nytimes.com/2005/11/09/business/09bank.html?_r=0*

OCC. (2002, December). Money laundering: A banker's guide to avoiding problems. Office of the Comptroller of the Currency. U.S. Department of the Treasury.

Washington, DC. Retrieved May 1, 2009, from *http://www.occ.treas.gov/moneylaundering2002.pdf*

OCC. (2002, September). Bank Secrecy Act/Anti-money laundering. *Comptroller's Handbook*. Comptroller of the Currency. Administrator of National Banks. Retrieved May 8, 2009, from *http://www.occ.treas.gov/handbook/bsa.pdf*

Paletta, D., Barrett, D., and Enrich, D. (2012, Aug. 15). Bank settles Iran money case. The Wall Street Journal (U.S. Edition). Retrieved December 1, 2012, from *http://online.wsj.com/article/SB10000872396390444318104577589380427559426.html*

Pozar, Z., Adrian, T., Ashcraft, A. and Boesky, H. (2010, Revised Feb. 2012). Shadow banking. Federal Reserve Bank of New York Staff Reports. Retrieved Dec. 15, 2013, from *http://www.ny.frb.org/research/staff_reports/sr458.pdf*

Reuter, P. and Truman, E. M. (2004). *Chasing dirty money. The fight against money laundering*. Washington D.C.: Institute for International Economics.

Rovella, D. E. and Baer, J. (2005). JP Morgan to pay $2 bln to settle WorldCom fraud suit. Bloomberg. Retrieved January 5, 2013, from *http://www.bloomberg.com/apps/news?pid=newsarchive&sid=auybDoZIEQTg*

Shadow banking system. (n.d.). Investopedia. Retrieved on January 15, 2013, from *http://www.investopedia.com/terms/s/shadow-banking-system.asp#axzz2LsObW2k4*

Sparshott, J. (2012, Dec. 10). Standard chartered settles U.S. sanctions allegations. *Wall Street Journal* (U.S. Edition). Retrieved January 5, 2013, from *http://online.wsj.com/article/SB10001424127887324478304578171150886564188.html*

The 40 Recommendations. (2003). FATF-GAFI. Retrieved May 1, 2009, from *http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html*

USA PATRIOT Act. (2001). Financial Crimes Enforcement Agency. US Department of the Treasury. Retrieved on May 1, 2009, from *http://www.fincen.gov/statutes_regs/patriot/index.html*

Watkins, R.C., Reynolds, K.M., DeMara, R.F., Georgiopoulos, M., Gonzalez, A.J., and Eaglin, R. (2003, January). Exploring data mining technologies as tools to investigate money laundering. *Journal of Policing Practice and Research: An International Journal. 4* (2): 163-178.

APPENDIX

Excerpts from FATF Recommendations

Role of the financial system in combating money laundering Customer Identification and Record-keeping Rules

10. Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names: they should be required (by law, by regulations, by agreements between supervisory authorities and financial institutions or by self-regulatory agreements among financial institutions) to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients, either occasional or usual, when establishing business relations or conducting transactions (in particular opening of accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, performing large cash transactions).
    In order to fulfill identification requirements concerning legal entities, financial institutions should, when necessary, take measures:
    (i) to verify the legal existence and structure of the customer by obtaining either from a public register or from the customer or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity.
    (ii) to verify that any person purporting to act on behalf of the customer is so authorised and identify that person.
11. Financial institutions should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are acting on their own behalf, for example, in the case of domiciliary companies (i.e. institutions, corporations, foundations, trusts, etc. that do not conduct any commercial or manufacturing business or any other form of commercial operation in the country where their registered office is located).
12. Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour. Financial institutions should keep records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the account is closed. These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.
13. Countries should pay special attention to money laundering threats inherent in new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes.

Increased Diligence of Financial Institutions

14. Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help supervisors, auditors and law enforcement agencies.
15. If financial institutions suspect that funds stem from a criminal activity, they should be required to report promptly their suspicions to the competent authorities.
16. Financial institutions, their directors, officers and employees should be protected by legal provisions from criminal or civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the competent authorities, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.
17. Financial institutions, their directors, officers and employees, should not, or, where appropriate, should not be allowed to, warn their customers when information relating to them is being reported to the competent authorities.
18. Financial institutions reporting their suspicions should comply with instructions from the competent authorities.
19. Financial institutions should develop programs against money laundering. These programs should include, as a minimum:
    (i) the development of internal policies, procedures and controls, including the designation of compliance officers at management level, and adequate screening procedures to ensure high standards when hiring employees;
    (ii) an ongoing employee training programme;
    (iii) an audit function to test the system.

Source: Customer due diligence for banks. (2001, Jan.). Bank for International Settlements. Retrieved December 15, 2009, from *http://www.bis.org/publ/*

KNOW YOUR CUSTOMER GLOSSARY

Beneficial Owner/IUB	Identification of Ultimate Beneficiary. The natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement. (http://www.fatf-gafi.org/dataoecd/42/43/33628117.pdf)
CIR	Client Identification Requirements. Information that is required or deemed necessary based on the customer's risk classification by the reporting entities. (http://www.aar.com.au/pubsaml/fmres/foamlmay06.htm)
ISF	Identification of Sources of Funds. Activities from which the funds came—legal or illegal employment, trust, another financial institution, etc..
PEPs	Politically Exposed Persons. Individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. (http://www.fatf-gafi.org/dataoecd/42/43/33628117.PDF)

http://www.fatf-gafi.org/pages/glossary/